AKADEMIA E FORCAVE TË ARMATOSURA
INSTITUTI KËRKIMOR SHKENCOR USHTARAK
REVISTË TEORIKO-SHKENCORE
SHTATOR 2024

REVISTA USHTARAKE

(edicioni i tretë)

INSTITUTI KËRKIMOR SHKENCOR USHTARAK © 2024

Botim i Akademisë së Forcave të Armatosura
Miratuar me vendim nr. 3, datë 23.09.2024
të Bordit Drejtues të Revistës Ushtarake

Bordi Drejtues i Revistës Ushtarake

Kryetari i bordit
Gjeneral Brigade **Bardhyl Nuredinaj**

Anëtarët e Bordit
Kolonel Msc. **Ulsi Rexhaj**
Prof. Asoc. Dr. **Etleva Smaçi**
Prof. Asoc. Dr. **Teki Kurti**
Kolonel (R) Dr. **Ahmet Leka**
Nënkolonel (R) Dr. **Enrik Ago**
Nënkolonel Dr. **Fitim Karasani**
Kolonel Msc. **Hysni Gjergji**

Përgatiti për botim: Grupi i Redaktimit dhe i Publikimit

Art design: Engjellushe Llulla

ISSN 2227-8133 (Print), ISSN 2227-8141 (Online)

Copyright © 2024 nga Instituti Kërkimor Shkencor Ushtarak në Akademinë e Forcave të Armatosura.

Akademia e Forcave të Armatosura zotëron liri akademike dhe respekton detyrimet ligjore të përcaktuara shprehimisht në ligjin për Arsimin e Lartë si dhe të gjitha aktet e tjera ligjore që janë të detyrueshme për institucionet publike.
Pikëpamjet dhe opinionet e shprehura në "Revista Ushtarake" janë të autorëve dhe nuk pasqyrojnë qëndrim zyrtar të Ministrisë së Mbrojtjes, Shtabit të Përgjithshëm të FARSH dhe Akademisë së Forcave të Armatosura. Autorët e shkrimeve nuk do të jenë subjekt i ndëshkimit për shprehjen e lirë të qëndrimeve dhe pozicioneve të tyre individuale, edhe sikur përmbajtja e tyre të mos jetë në përputhje me qëndrimet zyrtare të institucionit të mbrojtjes. Njëkohësisht, autori/autorët mbajnë përgjegjësi për shtrembërimet e fakteve si dhe kopjimet e pa referuara të krijimeve dhe mendimeve të autorëve të tjerë.

Akademia e Forcave të Armatosura
Instituti Kërkimor Shkencor Ushtarak
Shtypur: Shtator 2024

PËRMBAJTJA E REVISTËS USHTARAKE

RUBRIKA E PARË
Inteligjenca artificiale dhe zhvillimet inovative

Teknologjia kuantike dhe siguria e saj në fushën e informacionit........ 9
Kolonel Msc. Ulsi REXHAJ
Drejtor i Institutit Kërkimor Shkencor Ushtarak

Modernizimi i Forcave të Armatosura nën ndikimin gjeopolitik, dhe transformimin teknologjik... 29
Kolonel Msc. Hysni GJERGJI
Shef Departamenti në Institutin Kërkimor Shkencor Ushtarak

Rëndësia e dronëve në zbulimin dhe shuarjen e zjarreve.................... 45
Kolonel Msc. David RROKU
Zëvendësdrejtor i Institutit Kërkimor Shkencor Ushtarak

Siguria dhe qëndrueshmëria kibernetike e aviacionit. Vlerësimi i rrezikut në menaxhimin e trafikut ajror............................. 61
Laureta BETA
Specialiste në Drejtorinë e Trajnimit dhe Licencimit, ALBCONTROL

RUBRIKA E DYTË
Analiza dhe vlerësime për sigurinë dhe mbrojtjen

Impakti i luftës në Ukrainë në sistemin e sigurisë dhe mbrojtjes, kombëtare dhe kolektive.. 83
Kolonel (R) Msc. Dilaver HOXHA

Shërbimet e Inteligjencës të PMC dhe PSC, kërcënimi kryesor hibrid rus për, Ballkanin Perëndimor.. 101
Dr. Drizan SHALA
Lektor në Universitetin e Sarajevës

NATO në Ballkanin Perëndimor: Shqipëria nga "armiq" te motoja "miq besnik".. 111
Prof. Asoc. Dr. Etleva SMAÇI
Zëvendësrektor i Akademisë së Forcave të Armatosura

Lufta hibride, roli i teknologjisë dhe i inteligjencës artificiale.............. 125
Nënkolonel (R) Msc. Kanan HIMAJ

Ndërveprimi i fuqisë ajrore me inteligjencën ushtarake dhe sfidat e sigurisë.. 139
Major Sonila VARFI
Specialist në Drejtorinë e Radiozbulimit, AISM

RUBRIKA TRETË
Arsimimi dhe stërvitja në FA

Mbështetja logjistike e integruar në konceptin logjistik të NATO-s....... 153
Kolonel (R) Arben DHULI

Forca përmes dijes: Roli kyç i Edukimit Ushtarak Profesional në sigurinë kombëtare të Shqipërisë.. 163
Kolonel (R) Dr. Çlirim TOCI
Kolegji i Vendeve të Baltikut, Estonia

Krijimtaria dhe suksesi.. 175
Prof. Asoc. Dr. Edmond BRANESHI
Shef Grupi në Shkenca Komunikimi, FMS

Përgatitja dhe zhvillimi i oficerëve të sotëm për mënyrat e reja të luftës së nesërme.. 189
Nënkolonel (R) Msc. Besnik DACI
Specialist në Institutin Kërkimor Shkencor Ushtarak

Realiteti virtual dhe dobia e tij në Forcat e Armatosura....................... 197
Kryekapter Gëzim MATAJ
Nënoficer në Regjimentin e Operacioneve Speciale

RUBRIKA E PARË

INTELIGJENCA ARTIFICIALE DHE ZHVILLIMET INOVATIVE

Teknologjia kuantike dhe siguria e saj në fushën e informacionit

Kolonel Msc. Ulsi REXHAJ
Drejtor i Institutit Kërkimor Shkencor Ushtarak

Trajtesë e shkurtuar.

Mundësitë dhe aftësitë e sotme komunikuese, mendimi kritik, por dhe integrimi i teknologjisë kuantike në sistemet e sigurisë është bërë gjithnjë e më i përhapur në ruajtjen e të dhënave bazë, administrimin e informacionit, menaxhimin dhe qarkullimin e tyre. Në këtë material është përmbledhur ndikimi i teknologjisë kuantike, që bazohet në ligjet e fizikës mekanike kuantike në sigurinë kuantike, si një domosdoshmëri e kohës, pavarësisht kostove financiare.

Gjetjet tregojnë se format e ndryshme të teknologjisë klasike të përdorur deri më tani ndikojnë në rezultatet e sigurisë së ruajtjes së infrastrukturës kritike të të dhënave, informacionit dhe qarkullimit të tyre. Por angazhimi në mënyrë aktive në teknologjinë kuantike do të ketë një ndikim të thellë në përvojat e sigurisë kuantike, duke reflektuar motivim të shtuar, aftësi të përmirësuara të sigurisë dhe akses të përmirësuar në burimet bazë. Niveli i integrimit të kësaj teknologjie me atë klasike luan një rol të rëndësishëm në përcaktimin e rezultateve, duke u përdorur në mënyrë strategjike për të maksimizuar efektet e saj pozitive, me synimin për të debutuar në një botë të drejtuar nga teknologjia.

Fjalët kyçe: Teknologjia kuantike, siguria kuantike, siguria binare, ligjet e fizikës, enkriptrimi, sulm kibernetik, të dhëna, administrimi i informacionit, algoritme, protokolle, interferencë etj.

Hyrje

Ruajtja e rrjeteve dhe informacionit është një nga temat më të rëndësishme në lidhje me zhvillimet e sotme, konkurrencën afatgjatë dhe arritjen e sigurisë globale. Shprehja “siguri kuantike” rrjedh nga teknologjia kuantike që bazohet në ligjet e mekanikës kuantike, që do të thotë një funksion racional, integral, homogjen i dy ose më shumë ndryshoreve.

Siguria e rrjeteve dhe ruajtja e informacionit përfshin të gjitha masat që marrim për të parandaluar çfarëdo humbje të të dhënave apo ndërhyrje në rrjet. Të cilat mund të shkaktohen nga gabimet e shfrytëzuesve, defektet në kod, aktivitetet me qëllim dëmtimi, dështimi i harduerit apo dhe për shkaqe natyrore. Thënë dhe kuptuar më thjeshtë: siguria dhe masat për zbatimin e saj janë një domosdoshmëri imperative e kohës. Kjo përfaqëson procesin me anë të të cilit një domen, një produkt ose një shërbim ruhet, rinovohet dhe përditësohet duke aplikuar metoda të reja, duke futur teknika të bashkëkohore ose duke zhvilluar ide të suksesshme për të krijuar vlera të reja të organizimit të punës, shërbimit, menaxhimit etj.

Nëpër organizata dhe institucione ka shumë të punësuar që nuk i njohin çështjet e sigurisë sa e si duhet, prandaj ata mund të paraqesin rrezik në rrjedhjen e informatave dhe menaxhimin e rrjeteve. Sot nuk është vështirë të gjenden mjete, pajisje e programe të ndryshme, që në esencë janë konceptuar për qëllime të mira “për mbrojtjen dhe kontrollimin e rrjeteve”, por që hakerët apo sulmues të ndryshëm mund t’i përdorin për të depërtuar brenda rrjeteve të një organizate, institucioni apo në tërësinë e tyre për qëllime të ndryshme përfituese.

Inovacioni i teknikës mund të jetë një shtytës thelbësor i zhvillimit të sigurisë duke kërkuar që vazhdimisht të jemi më të suksesshëm, duke zëvendësuar teknologjitë klasike me teknologji kuantike dhe sigurinë nga klasike/binare në siguri kuantike. Për të qenë të suksesshëm, duhet të jemi në gjendje të identifikojmë mundësitë dhe të përfitojmë prej tyre. Vetëm nëpërmjet shqyrtimit dhe vlerësimit të sigurisë që kemi dhe të konstatimit se për çfarë sigurie kemi nevojë sot dhe në të ardhmen, do të mund të qëndrojmë përpara tendencave në rritje të saj, si dhe të jemi të gatshëm të eksperimentojmë me ide të reja.

Për mijëra vjet, kod-bërësit dhe shkelësit e kodeve kanë konkurruar për supremaci. Arsenalet e tyre kanë filluar të përfshijnë një armë të re të fuqishme: mekanikën kuantike. Kriptografia ose “arti i krijimit të kodeve” ka një histori të gjatë aplikimesh ushtarake dhe diplomatike, që datojnë që nga babilonasit. Në ditët e sotme, ajo po bëhet gjithnjë e më e rëndësishme në aplikacionet komerciale për biznesin elektronik dhe tregtinë elektronike. Të dhëna të ndjeshme të tilla si numrat e kartave të kreditit dhe numrat e identifikimit personal (PIN) transmetohen në mënyrë rutinore në formë të koduar. Mekanika kuantike është një mjet i ri, si për shkelësit ashtu edhe për krijuesit e kodeve, në garën e tyre të përjetshme. Ajo ka potencialin të revolucionarizojë kriptografinë si duke krijuar kode të sigurta të përsosura ashtu edhe duke thyer skemat standarde të kriptimit.

1. Teknologjia kuantike përdorimi në jetën e përditshme

Teknologjia kuantike është një klasë teknologjie që funksionon duke përdorur parimet e mekanikës kuantike (fizika e grimcave nën-atomike), duke përfshirë ndërthurjen dhe mbivendosjen kuantike.

Arsyeja pse po flasim për teknologjinë kuantike tani, 50 vjet pasi ajo u bë pjesë e jetës sonë përmes energjisë bërthamore, është se arritjet më të fundit të inxhinierisë po shfrytëzojnë më shumë potencialin e mekanikës kuantike. Kjo teknologji përdoret në sensorët dhe kompjuterët kuantikë duke u zhvilluar nëpërmjet inxhinierisë kuantike që bazohet në ligjet e mekanikës kuantike. Aktualisht, ka filluar të kontrollohet si ndërthurja ashtu dhe mbivendosja kuantike, duke e bërë atë një fushë magjepsëse që përdor parimet e fizikës kuantike për të krijuar mjete të reja dhe të fuqishme. Ndryshe nga teknologjia klasike përdoren grimcat në nivelin nën-atomik për të arritur gjëra që më parë ishin të paimagjinueshme. Kjo do të thotë se ajo premton përmirësime në një gamë të gjerë pajisjesh të përditshme, duke përfshirë:

- Sisteme më të besueshme të navigimit dhe kohës.
- Komunikime më të sigurta.
- Imazhe më të sakta të kujdesit shëndetësor përmes sensorit kuantik.
- Llogaritje më të sakta dhe më të fuqishme.

Më të përdorshme në jetën e përditshme janë:

- Magnetometri kuantik në mjekësi, që përdor efekte kuantike për të zbuluar ndryshimet më të vogla në fushën magnetike, p.sh., skanerët MRI (imazheri me rezonancë magnetike).
- Kriptografia kuantike në sigurinë e të dhënave, duke përdorur grimcat kuantike, si fotonet, për të transmetuar informacion, ajo siguron një nivel të lartë të sigurisë për të dhënat tona.

Teknologjia kuantike nuk është vetëm e ardhmja, por ajo tashmë është një realitet aktual që po ndryshon mënyrën se si ne kuptojmë dhe përdorim botën përreth nesh. Nëpërmjet aplikacioneve të sotme ne presim se çfarë do të sjellin hapat e ardhshëm në përparimin kuantik dhe si do të na çojnë në horizonte të reja. Të gjitha këto aplikacione, mund të jenë të dobishme në një kohë afatshkurtër, por është e vështirë të dihet se çfarë do të jetë një evolucion i vërtet dhe çfarë do të jetë shkatërruese. Kjo pasiguri na tregon se ndryshimi midis evolucionit dhe revolucionit ka të ngjarë të jetë një investimi i hershëm.

2. Siguria kuantike, dobishmëria dhe potenciali i saj

Siguria kuantike është një paradigmë e sigurisë në fushën e informacionit që përdor konceptet e fizikës kuantike për të siguruar komunikimin dhe shkëmbimin e informacionit në mënyrë të pazbulueshme dhe të paimagjinueshme nga agjentë të tretë, edhe pse ata mund të kenë kontroll mbi të dhënat në transmetim. Një nga mënyrat për të arritur këtë, është përmes përdorimit të kulturave kuantike të lidhura. Në këtë rast, komunikimi kuantik mund të bëhet përmes dritës së polarizuar që përfaqëson bit kuantike. Duke përdorur protokollet kuantike të sigurisë siç është protokolli BB84, informacioni është koduar në këto bit që mund të përfaqësojnë të dhëna të sigurta.

Gjithashtu një mënyrë tjetër është përmes bashkësisë së bërthamave të mbrojtura. Këtu, informacioni është koduar në gjendjet e një pajisjeje kuantike të përzgjedhur, për shembull, gjendjet e spin-it të një atomi ose fotoni. Gjatë komunikimit kuantik, nëse ndodh ndonjë përpjekje për të marrë apo shpërndarë informacionin nga një person i huaj, efekti i paprekshmërisë së informacionit kuantik do të bëjë që tentativa të ekspozohet. Kjo bazohet në ligjin e fizikës kuantike, që një përpjekje për të përfituar informacion nga një sistem kuantik do të ndikojë në gjendjen e tij.

Për të realizuar sigurinë kuantike në praktikë, janë të nevojshme teknologjitë e bashkësive kuantike, të cilat tashmë janë në zhvillim në laboratorët shkencorë në të gjithë botën. Këto teknologji synojnë të sigurojnë një mënyrë të paanshme dhe të sigurtë për të komunikuar në mes palëve, duke shfrytëzuar cilësitë e ngushta të fizikës kuantike për të siguruar integritetin dhe privatësinë e të dhënave.

Siguria kuantike është e dobishme sepse ajo na ofron:

Paprekshmëri të informacionit. Në sistemet kuantike, informacioni është i sigurt për shkak të karakteristikave kuantike të pajisjeve, duke bërë që tentativat për të ndërhyrë apo regjistruar informacionin të shfaqen.

Përçueshmëri e ndërhyrjeve apo kundërvajtjeve**.** Nëse një person i tretë tenton të regjistrojë ose të monitorojë një komunikim kuantik, efekti i paprekshmërisë ndikon në gjendjen e informacionit dhe tregon se ka ndodhur një ndërhyrje.

Siguri asimetrike. Në shumicën e protokolleve të sigurisë kuantike, pjesëmarrësit mund të shpërndajnë një qelb të sigurt të çelësave pa pasur dyshim për integritetin e tyre. Kjo krijon një mënyrë asimetrike të shpërndarjes së çelësave, që është e vështirë për të shfrytëzuar nga sulmuesit.

Eliminim të tentativave të shkeljes së sigurisë. Efekti i paprekshmërisë dhe i ruajtjes së informacionit kuantik mund të mposhtë tentativat për të shkelur sigurinë, duke bërë që sulmuesit të mendojnë dy herë para se të përpiqen të shfrytëzojnë një sistemi kuantik.

Siguri në nivelin fizik. Siguria kuantike është e bazuar në ligjet e fizikës kuantike, siç janë ato të super pozicionit dhe ndërveprimit të paprekshmërisë. Duke e bërë atë themel të sigurisë dhe të mos varur nga algoritmet e kompjuterit ose shkencat e tjera që mund të kenë kufizime të sigurisë.

Përdorim potencial për aplikacione të rëndësishme. Siguria kuantike mund të aplikohet në fusha të ndryshme ku siguria është kritike, siç janë: telekomunikacionet, bankat, sistemet e shëndetësisë dhe shkencat e kompjuterëve.

Për këto arsye, siguria kuantike ka potencialin për të ndryshuar paradigmat e sigurisë, duke i bërë ato që të mund të jenë më të sigurta dhe më të besueshme, për shkak të përfitimeve të saj unike nga karakteristikat e fizikës kuantike.

3. Siguria binare dhe dobësitë e saj

Siguria binare është një koncept që lidhet me sigurinë e të dhënave të dërguara dhe të ruajtura nëpërmjet sistemeve dhe protokolleve të bazuar në informacionin binar. Kjo përfshin mënyra të sigurimit të të dhënave të ndryshme, përfshirë të dhënat e enkriptuara, firmat digjitale, autentifikimin dhe kontrollin e qasjes. Ajo përdor mjete dhe metoda për të siguruar që programet të mos manipulohen dhe shfrytëzohen. Këto mjete nuk janë të pagabueshme, por kur përdoren së bashku dhe zbatohen siç duhet, ato mund të rrisin shumë vështirësinë e shfrytëzimit. Disa nga metodat që përdoren për sigurinë binare përfshijnë:

- ***Nuk ka ekzekutim (NX):*** Biti No eXecute ose NX, i njohur gjithashtu si parandalimi i ekzekutimit të të dhënave (DEP) shënon zona të caktuara të programit si jo të ekzekutueshme, që do të thotë se input-i ose të dhënat e ruajtura nuk mund të ekzekutohen si kod. Kjo pengon sulmuesit të jenë në gjendje të kalojnë te kodi i personalizuar i shellcodit që është i ruajtur në rafte ose në një ndryshore globale.
- ***Randomizimi[1] i shtrirjes së hapësirës së adresës:*** Adresa Space Layout Randomization (ASLR) është randomizimi i hapësirës në memorie ku janë programi, të dhënat e përbashkëta. Vështirëson sulmuesin të shfrytëzojë një shërbim, pasi njohuritë e tij nuk mund të ripërdoren ndërmjet nisjeve të programit.
- ***Mundësia e zhvendosjes vetëm për lexim:*** Zhvendosja vetëm për lexim (RELRO) është një masë sigurie që i bën disa seksione binare vetëm për lexim. Ekzistojnë dy "mode" të RELRO: e pjesshme dhe e plotë.
- ***Vendosja e lajmëruesve/reklamave (Canaries/Cookies):*** Stack Canaries janë një vlerë sekrete e vendosur në skedarë e cila ndryshon sa herë që

---

[1] Procesi i renditjes ose krahasimit ndaj njëri tjetrit i njerëzve, sendeve, çështjeve, provave etj.

programi fillon. Përpara kthimit të funksionit, ato kontrollohen dhe nëse duket se është modifikuar, dilet nga programi menjëherë. Kjo përcaktohet kur programi nis për herë të parë, që do të thotë se nëse programi ndahet, ai ruan të njëjtin grumbull të cookies, përmes një mekanizmi të njohur si "forking".

Por siguria binare ose siguria e bazuar në komunikim të zakonshëm të dhënash ka disa dobësi apo mangësi kryesore, pasi është vunerabël ndaj:

- ***Sulmeve kriptografike:*** Algoritmet e enkriptimit binar janë të rrezikuara nga sulme kriptografike si "bruteforce", analizë diferenciale, analizë të frekuencës, dhe të tjera që mund të shfrytëzojnë strukturën e algoritmeve të enkriptimit.
- ***Shfrytëzimeve të padëshiruara:*** Siguria binare mund të jetë e prekur nga sulmet e padëshiruara të kriptografisë, siç janë backdoors, weak key attacks, dhe sulmet e tjera që mund të përfitojnë nga dobësitë në implementimin e algoritmeve të enkriptimit.
- ***Zhvendosjes së informacionit:*** Informacioni i enkriptuar mund të bjerë në dorë të palëve të treta për shkak të humbjes së çelësave, keqpërdorimit të tyre, ose përdorimit të algoritmeve të dobëta të enkriptimit.
- ***Sulmeve për keqpërdorim nga personeli:*** Personeli i brendshëm që ka qasje në sistemet e sigurisë binare mund të jetë rrezik potencial për të zbuluar ose keqpërdorur informacionin e enkriptuar për qëllime të padëshiruara.
- ***Proceseve të rrugëtimit (qarkullimit) të informacionit:*** Informacioni i enkriptuar mund të jetë i rrezikuar gjatë transmetimit i të dhënave në rrjetet publike, ruajtja në serverë të treta, dhe shkëmbimi i tyre mes aplikacioneve të ndryshme.
- ***Protokolleve të komunikimit:*** Protokollet e komunikimit të zakonshëm mund të kenë dobësi të sigurisë që mund të shfrytëzohen për të kompromentuar të dhënat e transmetuara, duke përfshirë sulmet e "man-in-the-middle" dhe të tjera që ndikojnë në integritetin dhe konfidencialitetin e informacionit.

Për këto arsye, siguria binare nuk është e mjaftueshme për aplikacione që kërkojnë një nivel të lartë të sigurisë dhe privatësisë. Ndaj, përdorimi i teknologjive të sigurisë kuantike dhe paradigmat e tjera të sigurisë është bërë gjithnjë e më i preferuar për të garantuar mbrojtjen e të dhënave në ambientet e rriskuara të sotme të komunikimit dhe shkëmbimit të informacionit.

4. Siguria kuantike dhe siguria binare për sigurinë e informacionit elektronik

Siguria kuantike dhe siguria binare janë dy qasje të ndryshme për të siguruar informacionin në botën e kompjuterëve.

Siguria kuantike:

- Bazohet në principet e fizikës kuantike për të krijuar bërthama të mbrojtura, të cilat janë të paprekshme dhe të pakapshme.
- Përdor bërthama të mbrojtura për të bërë transferimin e informacionit në mënyrë të koduar, duke e bërë atë të pamundur për të prishur informacionin dhe të pazbulueshëm.
- Përfiton nga karakteristikat unike të materies në nivel kuantik, si polarizimi i dritës dhe entanglementi[2].
- Ofron një nivel sigurie që është praktikisht i pakapshëm për të depërtuar me metodat konvencionale.

Siguria binare:

- Bazohet në algoritme dhe protokolle të dizajnuara për të mbrojtur informacionin duke e enkriptuar atë në mënyra të caktuara.
- Përdor metoda të matematikës diskrete për të kriptuar dhe dekriptuar informacionin, duke përdorur algoritme të tilla si AES, RSA dhe shumë të tjera.
- Është e bazuar në kompleksitetin e algoritmeve kriptografike dhe në vështirësinë e faktorizimit të numrave të mëdha në matematikë.
- Në krahasim me sigurinë kuantike, siguria binare është e lëkundshme dhe mund të prishet nëse algoritmet e enkriptimit janë të prishur ose nëse ka ndonjë vonesë në përpunimin e tyre.

Dallimet ndërmjet sigurisë kuantike dhe sigurisë binare.

Dallimi kryesor mes tyre është në bazën, metodat dhe mjetet që përdor secila, por ka edhe disa dallime të tjera ndërmjet sigurisë kuantike dhe sigurisë binare:

- **Siguria e informacionit:** Siguria kuantike bazohet në parimet e fizikës kuantike dhe ofron një nivel absolut të sigurisë për shkak të karakteristikave unike të materies së vogël. Në anën tjetër, siguria binare është e bazuar në algoritme dhe protokolle matematikore dhe ofron një siguri të përshtatur sipas nivelit të kompleksitetit të algoritmeve dhe vlerës së çelësit të përdorur.
- **Shkathtësia e administrimit së informacionit:** Implementimi i sigurisë kuantike është më i vështirë dhe kërkon njohuri të thella në fizikën kuantive dhe teknologjinë e bërthamës së mbrojtur. Ndërsa, siguria binare është më e njohur dhe e lehtë për t'u kuptuar dhe për të implementuar për organizatat dhe komunitetet e IT-së.
- **Shkalla e përdorimit:** Siguria binare është përdorur gjerësisht në infrastrukturat digjitale të sotme, si interneti, bankat dhe komunikimet e biznesit.

---

[2] Ngatërrimi, pleksja

Nga ana tjetër, implementimi i sigurisë kuantike është ende në fazën e zhvillimit dhe është përdorur kryesisht në fusha shkencore dhe eksperimentale, megjithatë, po përgatitet për të përdorur në fusha të tjera në të ardhmen.

Këto dallime shfaqin natyrën dhe sfidat e ndryshme të secilës qasje për sigurimin e informacionit në botën e kompjuterëve.

5. Metodat dhe teknikat për të mbrojtur të dhënat nga dëmtimi dhe palët e treta

Kur flasim për sigurinë binare, referohemi në përgjithësi në metodat dhe teknikat e përdorura për të siguruar që të dhënat të jenë jo vetëm të padëmtuara por edhe të paarritshme për palët e treta të padëshiruara, këtu përfshihen:

- **Enkriptimi i të dhënave:** Procesi i ndryshimit të të dhënave në një formë të padeshifrueshme për të gjithë ata që nuk kanë çelësin për të shkëmbyer këtë informacion. Enkriptimi mund të përdoret për të mbrojtur konfidencialitetin e të dhënave nëpërmjet algoritmeve të ndryshme të enkriptimit.
- **Autentifikimi:** Sigurimi që një person ose një sistem është i identifikuar saktësisht përpara se të japë akses në të dhënat ose resurset e dëshiruara. Kjo mund të përfshijë përdorimin e fjalëkalimeve, certifikatave digjitale ose metoda të tjera të autentifikimit.
- **Kontrolli i qasjes:** Sigurimi që vetëm personat ose sistemet e autorizuar kanë qasje në të dhënat ose resurset specifike. Këtu përfshihet përdorimi i politikave të sigurisë, listave të bardha për të kontrolluar qasjen dhe teknologjitë e autentifikimit të bazuara në role.
- **Firmat digjitale**: Përdorimi i një shenje digjitale të dhënë për të verifikuar origjinën dhe autenticitetin e një dokumenti ose mesazhi. Mund të përdoret për të siguruar që një mesazh nuk është ndryshuar dhe vjen nga burimi i duhur.

Këto janë disa nga aspektet kryesore të sigurisë binare që përdoren për të mbrojtur të dhënat në rrjetet kompjuterike, komunikimet elektronike, dhe sistemet e shumta të informacionit që janë të ekspozuara ndaj rrezikut të keqpërdorimit ose sulmeve të ndryshme.

Sfidat dhe vështirësitë në aplikimin e sigurisë binare në teknologjinë kuantike.

Gjatë aplikimit të sigurisë binare në teknologjinë kuantike ndeshemi dhe me disa sfida e vështirësi, disa prej të cilave janë:

- **Kompleksiteti i protokolleve:** Protokollet e sigurisë kuantike janë të komplikuara dhe të vështira për t'u implementuar në praktikë. Duhen njohuri të thella të fizikës kuantike dhe të algoritmeve të sigurisë, si dhe aftësi për të zhvilluar pajisje të specializuara që komunikojnë në mënyrë kuantike.

- **Përshtatja me infrastrukturën ekzistuese:** Implementimi i sigurisë kuantike kërkon investime të konsiderueshme në infrastrukturë të re dhe pajisje të specializuara, apo dhe në integrimin e sistemeve me infrastrukturën ekzistuese.
- **Mungesa e standardizimit:** Në fushën e sigurisë kuantike, ende nuk ka një standard të përgjithshëm për protokollet dhe teknologjitë, krijohen vështirësi në zgjedhjen dhe implementimin e tyre.
- **Kufizimet teknologjike:** Teknologjitë kuantike janë ende në zhvillim dhe kanë kufizime të tyre në lidhje me distancën, shpejtësinë e transmetimit, dhe stabilitetin e pajisjeve. Vetëm për disa aplikacione bëhet i mundur implementimi i sigurisë kuantike.
- **Përpunimi i informacionit:** Informacionit kuantik kërkon një qasje të re në shkencën e kompjuterëve dhe në programim. Zhvillimi i algoritmeve të përshtatshme për përpunimin e tij është në fazat e hershme dhe akoma sfidues për programuesit dhe inxhinierët e software-it.
- **Siguria e qasjeve:** Arritja e sigurisë së qasjeve në sistemet kuantike do të thotë eliminim i ndikimit të interferencës së jashtme edhe përpjekjeve për të shkëputur apo të monitoruar komunikimin.

Për të adresuar këto sfida, është e rëndësishme për të gjithë komunitetin shkencor dhe industrial që të vazhdojnë të investojnë në zhvillimin e teknologjive kuantike, të krijojnë standarde dhe protokolle të përbashkëta për sigurinë kuantike.

Aplikimi i sigurisë kuantike në kompjuterët jo kuantikë.

Siguria kuantike përdor bërthamat e mbrojtura për të arritur një komunikim të koduar që nuk mund të prishet pa u diktuar. Për përdorimin e kësaj teknologjie, duhet të kemi pajisje që janë të afta për të përpunuar dhe kryer operacione të tjera kuantike nëpërmjet këtyre bërthamave.

Kështu që, nëse pajisjet që përdorim nuk janë kuantike, atëherë nuk do të jemi në gjendje të përdorim shërbimet e sigurisë kuantike që është një nga avantazhet kryesore të kërkimit në fushën e kompjutacionit kuantik, por për të përfituar prej saj, nevojiten pajisje specifike.

Lidhja ndërmjet teknikës klasike dhe asaj kuantike

- Teknika klasike dhe ajo kuantike janë dy qasje të ndryshme për të përshkruar dhe për të kuptuar botën dhe proceset e saj. Të dyja së bashku ndikojnë mbi shkencën dhe teknologjinë moderne në mënyra të ndryshme por kanë një lidhje të ngushtë mes tyre në disa aspekte:

- **Baza teorike:** Teknikat klasike dhe ato kuantike janë të ndërtuara mbi baza teorike të ndryshme. Klasikja bazohet në logjikën dhe matematikën klasike, ndërsa ajo kuantike përdor koncepte dhe principe të mekanikës kuantike.

- **Interpretimi i informacionit:** Teknika klasike përdor sisteme binare të bazuara në numrat 0 dhe 1 për të përshkruar dhe për të manipuluar informacionin. Ndërsa ajo kuantike përdor bërthamat e mbrojtura dhe gjendje kuantike për të përshkruar informacionin dhe për të manipuluar atë në mënyra të ndryshme.
- **Shpërndarja dhe shkëmbimi i informacionit:** Në teknikën klasike, informacioni shpërndahet dhe shkëmbehet nëpërmjet kanaleve të qartë të komunikimit. Në atë kuantike, informacioni është lidhur në mënyrë të pazakontë përmes bërthamave dhe qelizave kuantike, duke mundësuar transmetim të sigurt të informacionit.
- **Implementimi teknologjik:** Teknika klasike përdoret për të zhvilluar një gamë të gjerë teknologjish, duke përfshirë kompjuterët, telekomunikacionet etj. Ndërsa ajo kuantike përdoret për të zhvilluar teknologji të tilla si kompjuterët kuantike, sistemet e sigurisë kuantike etj.
- **Sfida dhe potenciale:** Teknika kuantike ofron disa përparësi në krahasim me atë klasike, duke përfshirë performancë më të lartë në disa aplikacione dhe siguri më të madhe në shumë kontekste. Megjithatë, ka edhe sfida në implementimin dhe përdorimin e teknologjisë kuantike, pasi në disa raste, teknika klasike mund të jetë më e përshtatshme ose më e lehtë për t'u përdorur.

6. Elementet e infrastrukturës për teknologjinë kuantike

Pavarësisht se teknologjia kuantike është një fushë e re dhe zhvillimi i saj është në vazhdim, deri tashmë janë krijuar disa elemente kyçe të infrastrukturës për këtë teknologji:

- **Qubit (bit kuantik):** Në një kompjuter kuantik, qubit është njësia bazë e informacionit në llogaritjen kuantike analogu i bitit në një kompjuter klasik. Ai mund të jetë në një gjendje superpozicioni të shumë gjendjeve të mundshme të bërthamës kuantike, duke ofruar potencialin për të përpunuar informacion në mënyra të avancuara.
- **Pajisjet shpërndarëse të çelësave kuantikë (Quantum Key Distribution - QKD):** Pajisjet e bërthamës së mbrojtur kuantike janë pjesa qendrore e infrastrukturës për shpërndarjen e çelësave kuantike. Nëpërmjet përdorimit të fenomeneve kuantike, si polarizimi i dritës dhe entanglementi, ato krijojnë një lidhje të sigurtë për të shkëmbyer çelës të koduar që mund të përdoren për një komunikim të sigurtë.

- **Pajisjet për përpunimin kuantik:** Janë pajisjet që lejojnë për të kryer operacione kuantike mbi qubit. Ato mund të jenë qubitët që janë të lidhur me njëri-tjetrin duke krijojnë bërthama të mbrojtura ose mund të jenë sisteme më të sofistikuara që ofrojnë aftësi të zgjeruara përpunimi.
- **Shërbimet e resë kuantike (cloud cuantik):** Kompanitë që ofrojnë shërbime të qasjes në *cloud* për kompjuterët kuantikë janë një element tjetër i infrastrukturës. Shërbimet e tyre japin akses të lartë për të përdorur pajisjet e kompjuterëve kuantikë dhe shpërndajnë të dhëna në mënyrë të sigurtë.
- **Algoritmet kuantike:** Zhvillimi i algoritmeve të përshtatura për kompjuterët kuantikë mundëson përdorimin e fuqisë së kompjuterëve kuantikë për të zgjidhur probleme të caktuara më me efikasitet në krahasim me kompjuterët klasikë.

Këto janë disa nga elementet thelbësore të infrastrukturës për teknologjinë kuantike, por zhvillimi i mëtejshëm i kësaj fushe do të sjellë ndryshime dhe shtesa të reja në të ardhmen.

Veçoritë e mjedisit të transmetimit për teknologjinë kuantike.

Mjedisi i transmetimit për teknologjinë kuantike është i rëndësishëm, pasi duhet të ofrojë përshtatshmëri, efektivitetit të shpërndarjes dhe komunikimit kuantik. Disa nga veçoritë kryesore të mjedisit të transmetimit për teknologjinë kuantike janë:

- **Përhapja e dritës:** Për shpërndarjen e bërthamave të mbrojtura, është e rëndësishme që drita të jetë në gjendje të përhapet në mënyrë të shkëlqyeshme në mjedisin ku është e instaluar pajisja. Mjediset me ndërprerje të vogla dhe përqendrime të ulëta të ndotësve janë me ideale për to.
- **Stabiliteti termik:** Pajisjet e teknologjisë kuantike duhet të kenë një temperaturë ambienti të stabilizuar. Luhatjet e mëdha të temperaturës mund të ndikojnë negativisht në performancën e tyre dhe mund të shkaktojnë humbje të informacionit.
- **Minimalizimi i ndërhyrjeve elektromagnetike:** Ndërhyrjet elektromagnetike mund të ndikojnë në saktësinë e rezultateve të operacioneve kuantike. Mjediset që ofrojnë një izolim dhe nuk lejojnë ndërhyrje janë më të preferuara.
- **Mbivendosja e informacionit:** Nëse informacioni që transmetohet është i ndjeshëm ndaj ndërhyrjeve të jashtme, është e rëndësishme të ketë mekanizma për të zvogëluar ose përjashtuar mbivendosjen e informacionit. Kjo mund të përfshijë teknika të ndryshme të kodimit të informacionit.
- **Sistemet e kryqëzimit të dritës:** Nëse përdoret drita për transmetimin e

informacionit kuantik, sistemet e kryqëzimit të saj janë të nevojshme për të lejuar shpërndarjen në mënyrë të qëndrueshme dhe të drejtpërdrejtë.

- **Siguria dhe privatësia:** Mjedisi i transmetimit duhet të garantojë sigurinë dhe privatësinë e të dhënave që po transmetohen, përfshirë mbrojtjen nga hakerët potencialë dhe shpërndarjen në mënyrë të sigurtë dhe të koduar.

Këto janë disa nga veçoritë e rëndësishme të mjedisit të transmetimit për teknologjinë kuantike. Sigurimi i një mjedisi të përshtatshëm të transmetimit është thelbësor për funksionimin e suksesshëm të pajisjeve dhe protokolleve të teknologjisë kuantike.

Mjediset e transmetimit për teknologjinë kuantike dhe atë binare.

Teknikat e transmetimit për teknologjinë kuantike dhe teknologjinë binare ndryshojnë në mënyrë të konsiderueshme. Ajo kuantike bazohet në principet e mekanikës kuantike dhe përdorin bërthama dhe gjendje kuantike për të transmetuar dhe procesuar informacionin, ndërsa teknologjia binare përdor sisteme të bazuar në përdorimin vetëm të numrave 0 dhe 1, për të koduar dhe transmetuar informacionin. Ndërkohë që teorikisht është e mundur që të përdoret i njëjti mjedis fizik për të dy teknologjitë, në praktikë, ka dallime të rëndësishme teknike dhe teknologjike. Disa nga dallimet kryesore janë:

- **Ndjeshmëria ndaj interferencës:** Teknologjia kuantike është shumë më e ndjeshme ndaj interferencës së jashtme dhe ndërveprimeve të mjedisit krahasuar me teknologjinë binare. Prandaj, është e nevojshme të mbrohen më mirë nga ndërveprimet e jashtme për transmetimet kuantike.
- **Struktura e protokollit:** Protokollet për transmetimin kuantik janë shumë të ndryshme nga ato për transmetimin binar. Ato përdorin mekanizma, menaxhim dhe bërthama që nuk janë të përdorura në teknologjinë binare.
- **Kosto dhe efikasiteti:** Teknologjia kuantike ende është në zhvillim dhe shpeshherë është më e kushtueshme dhe më pak efikase se teknologjia binare për shkak të nevojës për pajisje specifike dhe infrastrukturë të avancuar.

Pavarësisht se teorikisht mund të përdoret i njëjti mjedis fizik për të transmetuar të dhëna përmes teknologjive kuantike dhe atyre binare, në praktikë përdorimi i tyre do të kërkonte strategji të ndryshme të implementimit dhe infrastrukturë të veçantë për secilën prej tyre.

Pajisjet e mjedisit të transmetimit për teknologjinë kuantike.

Teknologjia kuantike është një fushë e përparuar shkencore që ka potencial të madh në shumë fusha, përfshirë edhe mjedisin. Disa pajisje që janë përdorur ose janë zhvilluar për të përdorur teknologjinë kuantike për të monitoruar dhe studiuar mjedisin përfshijnë:

- **Sensorët kuantikë:** Janë pajisje që përdorin qëllime kuantike për të detektuar ndryshime në mjedis. Kanë ndjeshmëri dhe të saktësi të madhe krahasuar me ata tradicionalë, mundësojnë monitorimin më të mirë të ndryshimeve në cilësinë e ajrit, ujit, dhe përmbajtjeve të ndryshme kimike.
- **Kriptografia kuantike:** Është një teknologji që përdor veçoritë e mekanikës kuantike për të siguruar komunikime të sigurta. Përdoret për të mbrojtur të dhënat mjedisore të ndjeshme, duke garantuar që informacioni i mbledhur për ambientin nuk mund të kapet ose ndryshohet nga palë të treta.
- **Komunikimi kuantik:** Teknologjitë e komunikimit kuantik përdoren për të siguruar transmetime të shpejta dhe të sigurta duke mbledhur dhe shkëmbyer të dhëna në kohë reale, monitorimin e zonave të vështira dhe në kohë të vështira.
- **Simulimet kuantike:** Nëpërmjet tyre mundësohet në modelimin dhe parashikimin e ndryshimeve mjedisore. Zgjidhja e problemeve komplekse mjedisore, kuptimi i impakteve të ndryshimeve klimatike ose proceseve natyroret mundësohen me përdorimin e kompjuterëve kuantikë.

Këto janë disa nga përdorimet potenciale të teknologjisë kuantike në fushën e mjedisit, dhe shpeshherë ekzistojnë përpjekje për të zhvilluar dhe përdorur teknologji të tjera që mund të ndihmojnë në mbrojtjen dhe monitorimin e mjedisit përmes ndërveprimeve kuantike.

Dobësitë e algoritmeve në sistemin binar.

Algoritmet matematikor të ndërtuara me sistemin binar përballen me një sërë dobësish ose sfidash të cilat mund të kufizojnë performancën e tyre në disa kontekste, siç mund të jenë:

- **Përfaqësimi i numrave të mëdhenj:** Edhe pse sistemi binar është i përshtatshëm për shumicën e aplikimeve, ai mund të ketë vështirësi në përfaqësimin e numrave të mëdhenj në një mënyrë efikase. Kjo çon në humbje të saktësisë ose nevojën për të përdorur struktura të avancuara për të përfaqësuar numrat.
- **Procedohet me numra të përkufizuar:** Në sistemin binar, numrat e algoritmeve përkufizohen në bazë të një numri të caktuar të bitave. Kjo mund të çojë në humbje të saktësisë për numrat e përcaktuar me shumë shifra pas presjes (pikë-decimal).
- **Operacionet me numra të rrumbullakosur:** Nëse duhet të punojmë me numra të rrumbullakosur në një shkallë të gjerë, sistemi binar mund të ketë sfida për të mbajtur saktësinë e numrit.
- **Kërkesat e memories:** Disa algoritme të ndërlikuara mund të kërkojnë

përpunim intensiv të numrave të mëdhenj, duke krijuar nevojën për kapacitet të madh të memories, për ruajtjen e numrave midis shkallëve të ndryshme të përpunimit.

- **Performanca e interpretimit të të dhënave:** Në disa raste, interpretimi i të dhënave të shprehura në sistemin binar mund të jetë më i ngadalshëm se interpretimi i të dhënave të shprehura në sisteme të tjerë numrash.
- **Kostoja e implementimit:** Implementimi i algoritmeve në sistemin binar mund të jetë me kosto efektive në disa raste, por në raste të tjera, mund të jetë më me leverdi të përdoret një sistem tjetër numërues për shkak të nevojave specifike të aplikacionit.

Këto dobësi ose sfida mund të analizohen në disa kontekste, veçanërisht në rastet kur është e nevojshme të përpunohen me saktësi numra të mëdhenj ose të punohet me numra të rrumbullakosur dhe kërkohet efikasitet i lartë. Për këto algoritmet mund të përdoren sisteme të tjerë numërues, siç është sistemi kuantik ose sistemet me numra të përkufizuar, të cilët janë më të përshtatshëm.

Sipas algoritmeve në sistemin binar, për të gjetur një artikull të veçantë midis N objekteve, sipas metodës klasike kërkohet të kontrollohet gjithë numri i artikujve nga 0 deri në N herë. Në vitin 1996 Lov Grover[3], shpiku një algoritëm kërkimi kuantik. Me algoritmin e tij, një kompjuter kuantik duhet të kërkojë vetëm një numër artikujsh nga 0 deri në √N herë.

Me ndërtimin e kompjuterit kuantik kjo do të mund të përdoret për të përshpejtuar rrënjësisht kërkimin shterues të çelësave, ndërsa pjesa më e madhe e kriptografisë konvencionale do të shpërbëhet.

7. Dizavantazhet e sigurisë kuantike

Siguria kuantike është një fushë e mbushur me potencial, por ka edhe disa sfida dhe dizavantazhe të cilat duhet të merren parasysh:

- **Infrastruktura komplekse:** Implementimi i sigurisë kuantike kërkon infrastrukturë të veçantë dhe komplekse, duke përfshirë pajisje specifike siç janë bërthamat apo qelizat kuantike, si dhe kanale të sigurta të komunikimit. Kjo krijon vështirësi dhe kosto për institucionet, organizatat dhe kompanitë në implementimin e saj.
- **Kosto e lartë:** Pajisjet dhe teknologjitë e nevojshme për sigurinë kuantike janë shpeshherë të kushtueshme për t’u blerë, implementuar dhe për të mirëmbajtur. Kjo mund të bëjë që përdorimi i tyre të jetë i papranueshëm për shumë nga përdoruesit e këtyre aplikacioneve.

---

[3] Lov Kumar Grover (born 1961) is an Indian-American computer scientist

- **Ndjeshmëria ndaj interferencës:** Teknologjitë kuantike janë shumë të ndjeshme ndaj interferencës së jashtme dhe ndërveprimeve të mjedisit. Kjo mund të bëjë që sistemet të jenë më të rrezikuar nga sulmet dhe përfitimet nga palë të treta.
- **Mungesë stabiliteti dhe qëndrueshmërie:** Duke qenë se këto teknologji janë ende në fazën e zhvillimit mund të kenë probleme me stabilitetin dhe qëndrueshmërinë. Prandaj implementimi i tyre mund të jetë më i zbatueshëm në aplikacione kritike.
- **Përfitimi nga zhvillimet në teknologji:** Ndërsa teknologjitë kuantike janë në zhvillim e sipër, ekziston një mundësi që sulmuesit të përfitojnë për të gjetur forma dhe mënyra për të thyer sigurinë kuantike. Kështu që sfidat për të mbajtur sistemet kuantike të sigurta dhe të aktuale janë prezente.
- **Standardet dhe ndërveprimi:** Për të përdorur teknologjitë kuantike në mënyrë efikase, është e nevojshme që të krijohen standarde të përbashkëta dhe që ato të jenë të ndërveprueshme midis tyre. Këto përbëjnë një sfidë tjetër të kësaj fushe ende në zhvillim dhe me shumë aktorë të ndryshëm në treg.

Vulnerabiliteti i sigurisë kuantike ndaj interferencës.

Siguria kuantike është përgatitur për të përballuar sfidat e interferencës, por nuk është e përjashtuar nga pa ndjeshmëria. Ka disa faktorë që mund të bëjnë që kjo siguri të jetë më pak efektive ndaj interferencës:

- **Mjedisi fizik:** Ndërveprimet me mjedisin fizik mund të ndikojnë në pajisjet dhe protokollet kuantike. Faktorët e jashtëm si radiacioni, fushat magnetike, dhe temperaturat e ndryshme mund të shkaktojnë shkëputje ose ndryshime në bërthamat kuantike, duke rrezikuar sigurinë e transmetimeve.
- **Sulmet e ardhura nga përdorues të brendshëm:** Në teori, sulmet e qëllimshme të realizuara nga përdorues apo administratorë të rrjeteve, duke përfshirë sulmet fizike dhe shfrytëzimin e ndërhyrjeve teknologjike të shpejta, mund të ndikojnë në sigurinë kuantike.
- **Ndërhyrjet njerëzore:** Veprimet njerëzore të tilla si sulmet fizike në infrastrukturën kuantike ose tentativat për të ndryshuar ose kapur informacionin gjatë transmetimeve kuantike rrezikojnë sigurinë.

Cenimi i sigurisë kuantike. Ekzistojnë disa elemente që mund të cenojnë sigurinë kuantike:

- **Teknikat e skanimit të parave:** Teknikat e përdorura për skanimin e parave mund të zbatohen për të kapur ose ndryshuar informacionin që transmetohet në kanale kuantike. Për shembull, një sulmues mund të përdorë një teknikë skanimi për të kapur një bërthamë kuantike dhe për të lexuar ose ndryshuar të dhënat që janë transmetuar nëpërmjet saj.

- **Sulmet nga brenda sistemit kuantik:** Sulmet e qëllimshme, të kryera nga palë që kanë qasje legjitime në sistemin kuantik, mund të ndikojnë në sigurinë e transmetimeve. Një administrator i sistemit mund të ndërhyjë në mënyrë të keqdashëse në pajisjet kuantike për të manipuluar të dhënat ose për të shkaktuar shkëputje të transmetimit.
- **Sulmet nga kompjuterët klasikë:** Kompjuterët klasikë gjithashtu mund të përdoren për të kryer sulme kundër sigurisë kuantike. Nëpërmjet tyre një sulmues mund të përballojë protokollet kuantike dhe të kërkojë një çelës privat nga një bërthamë e mbrojtur kuantike.
- **Moskomunikimi i plotë kuantik:** Në disa raste, moskomunikimi i plotë midis pjesëve të një sistem kuantik mund të krijojë me vetëdije ose pa dashje siguri të ulët. Kur ndodh moskomunikimi i plotë midis pjesëve atëherë ai mund të lejojë një sulmues të kapë informacion në mënyrë të padëshiruar dhe të dëmshme.

Këto janë disa nga elementet bazë që mund të cenojnë sigurinë kuantike. Është e rëndësishme që zhvilluesit dhe operatorët e sistemeve kuantike të marrin masat e nevojshme për të përballuar rreziqet potenciale dhe për të siguruar qëndrueshmërinë dhe sigurinë e tyre. Teknologjia kuantike përdor mekanizma të ndryshme për të minimizuar efektet e interferencës dhe për të garantuar sigurinë. Mund të përmendim protokollet kuantike që përdorin shpërndarjen kuantike të bërthamave të mbrojtura për të siguruar qëndrueshmërinë dhe sigurinë e transmetimeve. Shumica e sulmeve të mundshme ndaj sistemeve kuantike kërkojnë njohuri të thellë teknike dhe resurse të konsiderueshme, duke i bërë ato më të vështira për të realizuar. Është e rëndësishme të kuptohet se edhe pse teknologjia kuantike ofron siguri të përparuar, ajo nuk është e pamposhtur ndaj çdo lloj interference apo sulmi.

Cenimi i sigurisë kuantike nga pajisjet klasike.

Me gjithë nivelin më të lartë që ofron siguria kuantike, ajo mund të cenohet nga pajisjet klasike në disa raste. Kjo mund të ndodhë për shkak të disa faktorëve të cilët ndikojnë në integritetin dhe sigurinë e transmetimeve kuantike:

- Pajisjet klasike siç janë ato elektronike dhe elektromagnetike mund të shkaktojnë interferenca në pajisjet dhe proceset kuantike, e cila mund të çojë në humbje të të dhënave, ndryshime të papritura në transmetime ose dëmtim të pajisjeve kuantike.
- Sulmeve fizike duke përdorur mjete të forta elektromagnetike klasike ndaj pajisjeve kuantike mund të ndikojnë në sigurinë e transmetimeve kuantike duke dëmtuar pajisjet kuantike ose për të ndryshuar të dhënat që janë transmetuar.

- Individë me të drejtë përdorimi të rrjeteve nga pajisjet klasike, por që kanë qasje dhe në pajisjet kuantike mund t'i shfrytëzojnë për të manipuluar të dhënat ose për të krijuar siguri të dobët në transmetime.
- Në disa sisteme kuantike, moskomunikimi i plotë midis pajisjeve klasike dhe atyre kuantike mund të çojë në siguri të dobët ose të ulët, duke hapur rrugë për sulme të ndryshme apo manipulimin e të dhënave.

Megjithatë, ndryshe nga teknologjitë klasike, teknologjitë kuantike janë të dizajnuara për të përballuar dhe për të minimizuar efektet e këtyre rreziqeve. Në zbatim të protokolleve kuantike mund të përdoren teknika të sigurisë së avancuar për të mbrojtur transmetimet kuantike nga interferenca dhe sulmet potenciale. Megjithatë, është e rëndësishme që zhvilluesit dhe operatorët e sistemeve kuantike të jenë të vetëdijshëm për këto rreziqe dhe të marrin masat e nevojshme për t'i përballuar ato.

8. Përse duhet siguria kuantike, vlefshmëria dhe disa rekomandime

Siguria kuantike është e rëndësishme për shkak të asaj çfarë ajo ofron dhe mundëson ndër të cilat theksojmë:

- **Siguria e të dhënave:** Teknologjitë kuantike ofrojnë nivele të larta të sigurisë për transmetimin e informacionit. Përdorimi i koncepteve kuantike si shpërndarja e bërthamave të mbrojtura dhe të koduara kuantike siguron një mënyrë të sigurtë për të transmetuar dhe për të marrë të dhëna, duke u rezistuar sulmeve dhe kapjes së informacionit nga palë të treta.
- **Siguria e komunikimeve:** Siguria kuantike mundëson që transmetimet e informacionit të jenë të sigurta dhe të padeshifrueshme nga palë të treta. Kjo është veçanërisht e rëndësishme për komunikimet që përmbajnë informacion të ndjeshëm, siç janë të dhënat personale, financiare, apo të tjera.
- **Mbrojtja e infrastrukturës kritike:** Teknologjitë kuantike mund të përdoren për të mbrojtur infrastrukturën kritike, siç janë sistemet financiare, sistemet e telekomunikacionit dhe sistemet e sigurisë kombëtare, nga sulmet kibernetike dhe të tjera.
- **Përdorimi i sigurtë i kompjuterëve kuantikë:** Kompjuterët kuantikë janë të dizajnuar për të kryer llogaritje të shpejta e të avancuara, por gjithashtu janë të ndjeshëm ndaj sulmeve kibernetike, duke bërë që informacioni dhe llogaritjet që kryhen në këta kompjuterë të jenë të sigurta dhe të mbrojtura.
- **Siguria në telekomunikacione:** Pajisjet dhe protokollet kuantike mund të përdoren për të realizuar transmetime të sigurta të të dhënave në rrjetet e telekomunikacionit, duke garantuar që komunikimet e ndërmjetësuara përmes tyre janë të padeshifrueshme nga palë të treta.

Siguria kuantike është kritike për shumë aspekte të teknologjisë moderne dhe të shoqërisë në përgjithësi. Përdorimi i saj mund të ndihmojë në mbrojtjen e të dhënave dhe të infrastrukturës kritike nga sulmet dhe rreziqet e ndryshme.

Vlefshmëria e sigurisë kuantike krahasuar me shpenzimet financiare.

Vlerësimi i raportit të kostove financiare në raport me atë çfarë ofron siguria kuantike varet nga shumë faktorë, përfshirë kontekstin e përdorimit, nivelin e sigurisë që kërkohet dhe mundësitë financiare të organizatës institucionit apo individit. Në rrethana të caktuara, investimi në sigurinë kuantike mund të jetë më i leverdishëm dhe i justifikueshëm për shkak të përparimeve në aspektin e sigurisë që ofron. Disa argumente pse siguria kuantike mund të jetë e vlefshme janë:

- Ofron një nivel të lartë të sigurisë për transmetimet e informacionit. Nëse të dhënat e ndjeshme ose kritike duhet të mbrohen me kujdes të veçantë, investimi në sigurinë kuantike mund të jetë i arsyeshëm.
- Në disa fusha si financat, shëndeti, dhe siguria kombëtare ekzistojnë ligje dhe rregullore që kërkojnë nivele të larta të sigurisë për të dhënat dhe informacionin. Në këto raste, investimi në teknologji të tilla mund të jetë i nevojshëm për të përmbushur këto kërkesa ligjore.
- Nëse institucioni, organizata apo individi është i ekspozuar ndaj rreziqeve të larta kibernetike, investimi në siguri të avancuar mund të jetë një hap i rëndësishëm për të mbrojtur të dhënat dhe infrastrukturën e saj nga sulmet dhe shfrytëzimet e të tretëve.

Megjithatë, në disa raste, investimi në sigurinë kuantike mund të jetë i shtrenjtë dhe jo i justifikueshëm në raport me rreziqet dhe nevojat e organizatës apo institucionit. Është e rëndësishme të bëhet një vlerësim i kujdesshëm i kostos dhe përfitimeve përpara se të vendoset të investohet në sigurinë kuantike. Në shumë raste, përdorimi i teknologjive të sigurisë kuantike mund të jetë një zgjidhje e rëndësishme për të mbrojtur të dhënat dhe infrastrukturën nga rreziqet e rritura kibernetike, por duhet të merret parasysh një analizë e detajuar e kostos dhe përfitimeve përpara se të merret një vendim përfundimtar.

Disa rekomandime për ndryshime ligjore, protokollesh dhe rregullore për sigurinë kuantike

Në mënyrë të përgjithshme, për të promovuar dhe për të rritur sigurinë kuantike, mund të jepen disa rekomandime për ndryshime ligjore, protokollesh dhe të rregulloreve, ja disa prej tyre:

- **Standardizimi dhe certifikimi:** Krijimi i standardeve të qarta dhe proceseve të certifikimit për pajisjet dhe protokollet kuantike mund të ndihmojë në sigurimin e nivelit të duhur të sigurisë dhe në lehtësimin e përdorimit të teknologjive kuantike. Në mënyrë institucionale duhet të zhvillohen protokolle dhe procese për të vlerësuar dhe certifikuar pajisjet, protokollet kuantike dhe sigurinë e tyre.

- **Mbikëqyrja dhe zbatimi:** Është e rëndësishme që të ketë mekanizma mbikëqyrjeje dhe zbatimi për të garantuar që organizmat, institucionet dhe individët që përdorin teknologjitë kuantike të përmbushin standardet dhe rregulloret për sigurinë. Këtu përfshihen inspektimet, raportimin e incidenteve dhe masat disiplinore për ata që nuk përmbushin standardet e sigurisë.
- **Krijimi i politikave dhe procedurave:** Organizmat dhe institucionet duhet të hartojnë politika dhe procedura të qarta për përdorimin dhe menaxhimin e teknologjive kuantike në mënyrë që të sigurojnë që ato të funksionojnë në mënyrë të sigurtë dhe efektive. Këto politika dhe procedura mund të përfshijnë rregullat për qasje, mbrojtjen e të dhënave dhe trajnimin për personelin.
- **Bashkëpunimi ndërkombëtar:** Për të adresuar sfidat dhe rreziqet e sigurisë kuantike në nivel global është i rëndësishëm bashkëpunimi ndërkombëtar. Organizmat ndërkombëtare, siç është Organizata Ndërkombëtare për Standardizimin (ISO) dhe Interpoli, mund të luajnë një rol kyç në koordinimin e përpjekjeve për të promovuar sigurinë kuantike në nivel ndërkombëtar.
- **Investime në hulumtim dhe zhvillim:** Për të zhvilluar teknologji të reja dhe inovative për mbrojtjen e të dhënave dhe infrastrukturës është e nevojshme të investohet në hulumtim dhe zhvillim për teknologjitë kuantike, përfshirë sigurinë kuantike. Qeveritë, industria private, dhe institucionet akademike mund të bashkëpunojnë për të financuar dhe për të kryer studime dhe zhvillim në këtë fushë.

Përfundime

Duke përfunduar, teknologjia kuantike komplekse dhe inovative, ashtu siç është një përplasje e fortë, me atë klasike dhe koston financiare mund të bëhet një ndërmjetës i fortë i për sigurinë e të dhënave, informacionit dhe transmetimit të tij, si dhe infrastrukturës kritike. Është një mjet që u ofron studiuesve dhe zhvilluesve mundësi për të gjetur mjete, fakte dhe prova për të vërtetuar teoritë kuantive në lidhje me sigurinë. Nga ana tjetër përparimi i kësaj teknologjie mund të ndihmojë në krijimin e pajisjeve jetike për arritjen e qëllimeve akoma më komplekse. Në këtë mënyrë, mundësohet të pranohet bashkë-komunikimi i ndërsjellë midis shkencës dhe ligjeve të fizikës me teknologjinë kuantive, në aftësinë e tyre për të mbështetur zhvillimin te njëra-tjetra.

Është e rëndësishme të theksohet se integrimi efektiv i teknologjisë kuantive në sigurinë e të dhënave, komunikimit, informacionit, shpërndarjes dhe shfrytëzimit nuk duhet të ketë të bëjë thjesht me përdorimin e pajisjeve më të fundit, por edhe me përdorimin e teknologjisë kuantive si një mjet për të përmirësuar përgatitjen e individëve për sfidat dhe krijimin e kapaciteteve intelektuale dhe përdoruesve modern. Besojmë se ky zhvillim nuk do të ketë të ndalur, shkenca premton shumë për të ardhmen, ashtu si kundër sot inteligjenca artificiale, pra sisteme eksperte që zhvillojnë një dialog me përdoruesin, tani është një fakt.

Bibliografia

1. Daniel Gottesman & Hoi-Kwong Lo "From Quantum Cheating to Quantum Security"
2. J. Preskill, "Battling Dekoherence: The Fault-Tolerant Quantum Computer"
3. B. Schneier, Applied Cryptography (2nd ed., Wiley, New York, 1996)
4. L. K. Grover, "In Proc. of the 28th Annual ACM Symposium on the Theory of Computing (STOC), (ACM Press, New York, 1996).
5. E. Biham, "In Proc. of the 31th Annual ACM Symposium on Theory of Computing" (STOC) (ACM Press, New York, 2000).
6. https://www.binarysecurity.no/
7. https://www.paconsulting.com/insights/what-is-quantum-technology
8. http://www.physicstoday.org/pt/vol-53/iss-11/p22.html c 2000
9. http://www.odci.gov/csi/books/venona/preface.htm

Modernizimi i Forcave të Armatosura nën ndikimin gjeopolitik dhe transformimin teknologjik

Kolonel Msc. Hysni GJERGJI,
Shef Departamenti në IKSHU

Trajtesë e shkurtuar.

Punimi ka synim të sjellë për lexuesin ushtarak udhëtimin transformues të NATO-s përmes transformimit teknologjik dhe digjital, si faktori kryesor modernizues. Në samitin e Uashingtonit në korrik 2024 u arrit në përfundimin se deri në vitin 2030, modernizimi dhe transformimi digjital i NATO-s do t'i lehtësojë operacionet në shumë fusha të aleancës, duke siguruar ndërveprueshmëri, rritje të ndërgjegjësimit dhe vendimmarrje të bazuar në më shumë të dhëna. Në frymën e zhvillimeve teknologjike përtej vitit 2025, punimi pasqyron qasjen, nivelin dhe rëndësinë që ka pësuar modernizimi i forcave të armatosura, nga luftërat botërore deri në epokën e inteligjencës artificiale.

Ky punim është bazuar në gjetjet më të mira të instituteve të shteteve aleate që përcaktojnë dhe paraqesin parimet e modernizimit të forcave të armatosura, duke prezantuar kuptimin praktik dhe tendencat e së ardhmes së konceptit DOTMLPF-P. Për përgatitjen e këtij materiali shkencor janë bërë hulumtime në rolin e pazëvendësueshëm që kanë pasur disa nga personalitetet më të larta të ushtrisë në shekuj, si, Hans von Seeckt, shef i shtabit të përgjithshëm të ushtrisë gjermane gjatë Luftës së Parë Botërore, si dhe drejtuesit më të lartë të ushtrisë dhe shtetit amerikan George Marshall, Dwight Eisenhower, George Paton etj.

Modernizimi përmbushet dhe kryhet me sukses, kur iniciativat e digjitalizimit aktual dhe progresiv janë të zbatuara me sukses në të gjithë komponentët e

DOTMLPF-P dhe rrisin aftësinë e FA-ve për të përmbushur misionin e saj. Ky punim do të ndihmojë studentët ushtarakë, kursantët e kolegjit dhe ushtarakët e tjerë të mësojnë dhe të zhvillojnë një kuptim më praktik të modernizimit të ushtrisë nga shembujt historikë deri në kushtet e transformimeve digjitale dhe ndryshimeve gjeopolitike. Për më tepër, trajtimi i mëposhtëm është i vlefshëm në epokën bashkëkohore të çështjeve të paqëndrueshme të sigurisë kombëtare, rajonale dhe globale, të ndërlikuara, si dhe nga kufizimet e burimeve të mbrojtjes.

Parë në këtë kontekst, gjykoj se ky punim do të jetë e dobishme për ushtarakët profesionistë që do të bashkohen në procesin e modernizimit të ushtrisë, si dhe do të ndihmojë në përpjekjen e pandërprerë të MM për të transformuar në mënyrë progresive FA të RSH.

Fjalët kyçe: DOTMLPF-P, NATO, RAND, modernizim, doktrinë, lidership, trajnim, organizim, elemente kritike.

1. Teoria e modernizimit dhe korniza DOTMLPF-P

Për të ruajtur avantazhin e saj përballë fuqive ushtarake armike, forcat e armatosura të çdo shteti duhet të modernizohen dhe të prodhojnë më shumë aftësi luftarake, trajnime bashkëkohore dhe ndërveprueshmëri përmes operacioneve me shumë domene. Çfarë është modernizimi i forcave të armatosura? Është transformimi progresiv i elementeve kritike me anë të të cilave forca e armatosur përcakton, ndërton dhe vepron sipas kornizës: Doktrina, Organizimi, Trajnimi, Materiali, Udhëheqja dhe Arsimi, Personeli. Në mënyrë të veçantë, modernizimi zhvillohet kur sipërmarrjet e transformimit progresiv, të zbatuara me sukses në të gjithë komponentët DOTMLPF-P, i rrisin aftësitë e FARSH për të përmbushur misionin e saj.

Analiza e këtij përkufizimi të modernizimit dhe e kornizës DOTMLPF-P tregon kohezionin kolektiv për të lehtësuar dialogun në planifikimin dhe ekzekutimin e modernizimit të ushtrisë në rang kombëtar dhe në kuadër të aleancës. Përkufizimi i mëparshëm i modernizimit ndikohej nga literatura mbi teorinë e modernizimit dhe nga të kuptuarit se elementet e kornizës DOTMLPF-P përcaktojnë së bashku se si FA-të zhvillohen dhe veprojnë. Literatura mbi teorinë e modernizimit, në veçanti kontributi i Seymour Lipset[1] dhe WW Rostow[2], është vlerësuar si jashtëzakonisht i dobishëm dhe me ndikim. Punimet e këtyre dy studiuesve janë thelbësore për teorinë e modernizimit, e cila synon të promovojë të kuptuarit se si evoluojnë shoqëritë njerëzore.

Seymour Lipset, në *Political Man: The Social Bases of Politics*, e shikon dhe analizon modernizimin e shoqërive njerëzore në varësi të zhvillimit të demokracisë. Ai shqyrton teoritë tradicionale se si demokracia evoluon në një shoqëri përmes analizës empirike të faktorëve shkaktarë, që janë arsimi dhe ekonomia. Qasja e S. Lipset tregon përdorimin që ne i bëjmë kornizës DOTMLPF-P për të studiuar dhe kuptuar modernizimin e ushtrisë. Ndërsa W.W. Rostow, në librin e tij, *Fazat e rritjes ekonomike*, thekson se shoqëritë modernizohen duke përparuar në disa faza të rritjes socio-ekonomike dhe të ndikuar nga politika. Rostow i identifikon këto faza si: shoqëria tradicionale; kushtet paraprake për periudhën e ngritjes; ngritja; procesi i maturimit; dhe maturimi përfundimtar.

---

[1] https://cis.ethz.ch/content/dam/ethz/special-interest/gess/cis/cis-dam/CIS_DAM_2015/WorkingPapers/Living_Reviews_Democracy/Wucherpfennig%20Deutsch.pdf

[2] https://godsonug.files.wordpress.com/2018/09/session-41.pdf

Me teorinë e Rostow, ne mund të kuptojmë dinamikën e shkakut dhe ndikimit që formëson modernizimin e ushtrisë. Teoria e modernizimit e lehtëson analizën intelektuale se si shoqëritë evoluojnë politikisht dhe socio-ekonomikisht. Me kalimin e kohës, teoricienë të ndryshëm kanë identifikuar dhe argumentuar se çfarë e përbën modernizimin e shoqërive njerëzore, duke filluar që nga shkaqet, trajektorja e ndryshimit, fazat e ndryshimit dhe implikimet e faktorëve të tjerë. Megjithatë, ajo që unë vlerësoj të dobishme për rastin e Shqipërisë dhe FA të RSH, është pikëpamja e pranuar përgjithësisht e modernizimit si një tranzicion progresiv, nga e tashmja në të ardhmen të aspekteve të ndryshme, si gjeopolitike, ekonomike, shoqërore, ushtarake etj. Teoria e modernizimit ofron bazën teorike për të kuptuar se FA-të, si pjesë e shoqërisë njerëzore, evoluojnë dhe modernizohen në mënyrë progresive. Korniza e transformimit DOTMLPF-P është një qasje efektive që FA-të, në të gjithë aleancën dhe jo vetëm në Shqipëri, përdorin për të konceptuar, planifikuar dhe zbatuar ndryshimet organizative. Nevojat e modernizimit ose ndryshimit të zbatuara në të gjithë komponentët DOTMLPF-P, do t'i mundësojnë edhe FA të RSH të evoluojë në mënyrë cilësore.

2. Doktrina si tërësia themelore e parimeve dhe nënkomponent i strategjisë ushtarake

Doktrina ushtarake përbëhet nga parime që e drejtojnë planifikimin dhe zbatimin e gamës së misioneve që një degë, armë apo shërbim i caktuar në FA mund të urdhërohet për të kryer. Sipas RAND[3]-it, doktrina ushtarake është "tërësia themelore e parimeve që udhëheqin FA-të për të përmbushur objektivat e sigurisë kombëtare . Studiuesi i çështjeve ushtarake, Barry R. Posen[4], e përshkruan doktrinën, si "një nën komponent të strategjisë së madhe që merret në mënyrë eksplicite me instrumentet ushtarake". Ndërsa strategjia e sigurisë kombëtare është mënyra se si një shtet planifikon të mbrojë veten dhe interesat e tij, doktrina nga ana e saj, e udhëzon se cilat mjete ushtarake të duhura do të përdorë forca e armatosur dhe si do t'i monitorojë ato mjete. Si qasje normative ndaj operacioneve luftarake, doktrina ndikon në strukturën organizative, trajnimin dhe pajisjen e një institucioni ushtarak, por mund të ndodhë e kundërta. Me fjalë të tjera, një komponent i kornizës së modernizimit DOTMLPF-P mund të nxisë modernizimin, ndërsa ndryshimet në aspekte të tjera të kornizës mund të nxisin ndryshime doktrinare. Doktrina nxit modernizimin përmes analizës dhe studimit të konfliktit të mëparshëm, mësimeve të nxjerra, analizës së kërcënimit, kërkesave operacionale, si dhe përmes eksperimentimit në degë të ndryshme të një shërbimi në Forcat e Armatosura.

---

[3] https://www.pbs.org/wgbh/americanexperience/features/nash-rand/

[4] https://www.foreignaffairs.com/authors/barry-r-posen

Gjatë viteve ndërmjet Luftës së Parë dhe të Dytë Botërore, ushtria gjermane ilustroi një rast të ndryshimit doktrinar, i cili nxiti modernizimin e ushtrisë. Në Reichswehr[5], reforma doktrinare buronte nga një analizë dhe studim i përqendruar i luftës, i profesionit të armëve dhe i eksperimentimit të guximshëm. James Corum[6] shkruan se shtabi i përgjithshëm gjerman kishte traditën më të fortë dhe më të mirë të studimit të luftës në mënyrë kritike, duke ofruar analiza objektive të operacioneve ushtarake. Në përputhje me traditën, oficerët gjermanë studiuan dhe shkruan gjerësisht jo vetëm mbi sukseset, por edhe mbi gabimet strategjike, operacionale, taktike dhe teknologjike të bëra gjatë Luftës së Parë Botërore.

Shefi gjerman i Shtabit të Përgjithshëm Hans von Seeckt[7], i emëruar në vitin 1920, besonte se Lufta e Parë Botërore vërtetoi se manovra ishte superiore ndaj fuqisë së zjarrit dhe e përfytyronte luftën e ardhshme si një çështje manovrimi të mekanizuar. Hans von Seeckt fokusoi një pjesë të konsiderueshme të Korpusit të Oficerëve të Ushtrisë në studimin e Luftës së Parë Botërore dhe në eksplorimin e ideve për përmirësimin e doktrinës së manovrimit duke përdorur teknologji të re. Ai emëroi mbi katërqind oficerë me përvojë luftarake, që ishin afërsisht 10 për qind e oficerëve të organizuar në komitete të ndryshme, për të studiuar doktrinën dhe taktikat e Luftës së Parë Botërore. Kjo rezultoi në hartimin e Rregullores së jashtëzakonshme të Ushtrisë, të titulluar "Udhëheqja dhe Beteja me Armët e Kombinuara". Kjo rregullore ndryshoi fokusin e doktrinës gjermane nga manovra mbrojtëse në atë sulmuese, si dhe reformoi me guxim formacionet, manovrat dhe taktikat e njësive ushtarake.

Me fjalë të tjera, një forcë (FT, FD, FAj) mund të identifikojë aplikime shtesë më të hollësishme të një inovacioni ekzistues teknologjik, si dhe të zhvillojë doktrinën për të shfrytëzuar aftësitë e këtij zhvillimi inovativ. Ky ishte rasti me teknologjinë e helikopterëve dhe zhvillimin e doktrinës ajrore në ushtrinë amerikane, e cila përdori helikopterë gjatë Luftës së Koresë kryesisht për transport dhe për evakuim mjekësor. Pas luftës së Koresë, u vlerësua se teknologjia e helikopterëve mund të shfrytëzohej për manovra luftarake, përveç mbështetjes logjistike. Në lidhje me këtë, gjenerallejtënant James Gavin[8], i cili më parë komandonte Divizionin e 82-të Ajror në Luftën e Dytë Botërore, vlerësoi se roli i mbështetjes logjistike të helikopterëve duhet të jetë dytësor, krahasuar me manovrën taktike luftarake. Në përputhje me propozimin, vlerësimin dhe analizën e Gavin, në mars 1955, ushtria amerikane botoi doktrinën që u quajt, *Qarkorja e Trajnimit 1-7: Përdorimi i Aviacionit të Transportit Ushtarak*. Ky botim doktrinar shprehte se roli i "aviacionit të transportit të ushtrisë ishte të lëvizte njësitë luftarake të forcave të armatosura në mënyrë operative nga ajri".

---

[5] https://kids.britannica.com/students/article/Reichswehr/334371

[6] https://securityanddefence.pl/Author-James%20S.-Corum/110229

[7] https://nla.gov.au/nla.cat-vn981506

3. Organizimi, struktura përbashkuese e individëve të ndryshëm për misionin e përbashkët

Komponenti organizativ i kuadrit DOTMLPF-P i referohet burimeve njerëzore, të mbështetura financiarisht brenda një force apo shërbimi, që janë ngritur për të përmbushur një mision specifik. Sipas modelit të SHBA, ky komponent i përket një njësie ose elementi të përbashkët me funksione të ndryshme nga një strukturë përmes së cilës individët bashkëpunojnë për të përmbushur misionin e përbashkët luftarak.

Ashtu si te doktrina, një ndryshim progresiv në FA mund të nxisë modernizimin në të gjithë kornizën, por ndryshimi mund të burojë dhe nga modernizimi brenda elementeve të tjera të kornizës. Me fjalë të tjera, FA-të ndonjëherë bëjnë ndryshime organizative në personel për të nxitur modernizimin dhe ato do të bëjnë ndryshime organizative në përgjigje të zhvillimeve të doktrinave.

Hans von Seeckt, në kohën që drejtonte shtabin e përgjithshëm gjerman, ndërmori reforma organizative për të krijuar grupin e talenteve intelektuale të oficerëve, me qëllim modernizimin e ushtrisë përmes përvojës dhe aftësive të tyre teorike dhe ushtarake. Ai përfshiu rindërtimin dhe bashkimin e strukturave vartëse brenda ushtrisë dhe ruajti funksionet thelbësore, jetike për modernizimin e ushtrisë. Megjithëse Traktati i Versajës i kërkonte atij shpërbërjen e Shtabit të Përgjithshëm Gjerman, von Seeckt ruajti stafin e trajnuar dhe i shpërndau në strukturat që ai vlerësonte si të domosdoshme. Seksionet e tjera të Shtabit të Përgjithshëm të vjetër thjesht u transferuan në departamente të tjera, por asnjëherë nuk u hodhën poshtë, si burime njerëzore më shumë vlera.

Në përpjekjet e tij për të shfrytëzuar talentin intelektual në ushtrinë gjermane, Von Seeckt miratoi kriteret intelektuale dhe profesionale për reduktimin e forcës në favor të mbajtjes së talenteve të spikatur. Ai këmbëngulte të kishin përparësi anëtarët e Korpusit të Shtabit të Përgjithshëm për shkak të përvojës së tyre në organizimin dhe planifikimin luftarak në vite. Përpjekjet e tij për riorganizim ndihmuan Gjermaninë të modernizohej duke ruajtur dhe përqendruar kapitalin intelektual njerëzor të disponueshëm në transformimin progresiv të doktrinës dhe komponentëve të tjerë të kornizës së modernizimit. Zbatimi i kapitalit intelektual në zhvillimin doktrinar çoi në zhvillimin dhe botimin e doktrinës së titulluar, *Udhëheqja dhe Beteja me Armët e Kombinuara*.

---

[8] https://www.uso.org/stories/188-james-m-gavin-a-legend-and-a-leader

Ky ndryshim në doktrinë solli gjithashtu ndryshime në strukturën e formacioneve të njësive të ushtrisë si dhe rriti aftësinë e tyre të manovrimit, zjarrit dhe inteligjencës. Institucioni e përmirësoi konstruktin e personelit dhe pajisjeve duke rritur sasinë e artilerisë së motorizuar dhe mundësitë për zbulim në thellësi të kundërshtarit, rritjen e artilerisë së lëvizshme, forcat e zbulimit, infrastrukturën e komunikimit dhe avionët e vëzhgimit. Shembujt historikë të luftërave dhe historisë së ushtrive në vite tregojnë se një ushtri mund të bëjë ndryshime progresive organizative për t'u modernizuar, transformuar në komponentët e tjerë të DOTMLPF-P, por mund të nxisë gjithashtu edhe ndryshime në strukturat organizative brenda saj.

Në rastin e FARSH, përvojat dhe mësimet e nxjerra të përmendura më lart duhet të zbatohen në drejtim të mbajtjes në shërbim të oficerëve të trajnuar dhe të talentuar, përtej absurditetit të ligjit për pushtetet dhe autoritetet, që nuk i lejon të dalin në pension. Ekspertiza e oficerëve të veçantë në FARSH nuk mund të krijohet pa përvojë dhe qëndrimi për një kohë të gjatë në shërbimin ushtarak. Cilësia e projekteve, koncepteve, dokumenteve, doktrinave dhe manualeve do të jetë e varur nga ata të cilët i përgatisin.

4. Trajnimi, procesi që vetëm përditësohet dhe asnjëherë nuk përfundon në karrierën ushtarake

Komponenti i trajnimit si komponent i kornizës së modernizimit DOTMLPF-P meriton një vend të rëndësishëm, sepse është integral dhe përbashkues në normalizimin e ndryshimit në komponentët e tjerë. Trajnimi është plotësim i njohurive dhe aftësive që i nevojiten personelit ushtarak për të kryer detyrat e tyre, me qëllim funksionimin me sukses të forcës së caktuar, si dhe përmbushjen e misionit të kësaj force, e cila i nënshtrohet trajnimit. Nuk mund të ketë ndryshim të qëndrueshëm dhe evoluim cilësor në doktrinë, organizim, pajisje ose materiale pa përshtatjen dhe përditësimet e suksesshme të metodave të reja të trajnimit, në për përmbushjen e misionit të FARSH. Pamundësia për t'u përshtatur në komponentin e trajnimit do të dëmtojë ndryshimet në doktrinë, organizim dhe pajisje, për shkak të ndikimit në misionin e FA-ve.

Përditësimi dhe evoluimi i trajnimit drejtohet dhe zhvillohet nga ndryshimet progresive në doktrinë, materiale dhe pajisje. Adaptime të tilla zakonisht kërkojnë që FA të stërviten dhe të zhvillojnë aftësitë e tyre, bazuar në modele të reja të përcaktuara nga doktrina dhe në pajisjet e reja të prezantuara. Shembull nga historia është rasti i ushtrisë amerikane, e cila për të ruajtur efektivitetin operacional në integrimin e doktrinës air mobile dhe helikopterëve, iu desh të ritrajnonte personelin ushtarak me përshtatje stërvitore, të cilat do të ishin thelbësore për suksesin e njësisë në betejën e vitit 1965 te Lugina e Drangit.

Rëndësia e komponentit "trajnim" ilustrohet në mënyrë të hollësishme nga modernizimi gjerman gjatë periudhës ndërmjet luftërave, 1919-1933. Drejtimi me mision është termi i përdorur për të përshkruar «vendimin e decentralizuar» të drejtimit me mision nga vartësit duke përdorur të ashtuquajturën «iniciativë të disiplinuar» dhe veprim të pavarur. Ushtria gjermane në këtë periudhë trajnoi drejtues ushtarakë në të gjitha nivelet për të menduar dhe gjetur zgjidhje të duhur brenda kornizës të misionit. Përmes kësaj risie udhëheqësit ushtarakë u vlerësuan si burra me mendim, vizion dhe veprim të pavarur si kur japin ashtu edhe kur marrin urdhra. Elasticiteti mendor ishte qëllimi kryesor i oficerëve dhe qasje e re ndaj stërvitjes dhe trajnimit, që do të kërkonte udhëheqës luftarakë dhe vizionarë, të cilët do të merrnin "iniciativën e disiplinuar" për të përmbushur qëllimin e komandantëve të tyre.

Aftësimi dhe trajnimi fizik është një nga fushat për të ruajtur gatishmërinë, rezistencën dhe moralin gjatë stërvitjeve të gjata verore dhe dimërore, në kufijtë e qëndrueshmërisë dhe mbijetesës fizike. Në rastin e Forcave të Armatosura të Republikës së Shqipërisë, mendoj se trajnimi individual poshtë nivelit të kompanisë për të ndërtuar një bazë të fortë njohurish taktike midis drejtuesve të rinj duhet të jetë një nga objektivat e trajnimit të personelit tonë në FA. Programi i trajnimit të njësive të vogla, skuadrat, togat dhe kompanitë në përputhje me rregulloret e këmbësorisë së aleancës, mendoj se duhet të përshtatet vazhdimisht me ato në Forcat tona Tokësore, veçanërisht. Një nga manualet më të rëndësishme që mendoj se duhet të aplikohet në Akademinë e Forcave të Armatosura, për programet e oficerit të ri, është *Stërvitja në Nivel Taktik,* edhe si përgjigje e luftërave të parregullta dhe hibride të cilat drejtohen dhe ekzekutohen nga formacione të vogla.

5. Materialet dhe revolucionarizimi teknologjik i pajisjeve dhe teknologjisë ushtarake

Komponenti material i kornizës DOTMLPF-P fokusohet në pajisjet e nevojshme që FA-të janë mbështetur për të kryer me sukses misionin e tyre. Ky komponent ka një lidhje të fortë me komponentët e tjerë DOTMLPF-P, gjë që e bën të rëndësishëm vendin e tij në këtë kornizë. Teknologjia dhe revolucionarizimi shkencor i materialeve[9] ndikojnë në ndryshime në doktrinë, organizim, trajnim dhe komponentë të tjerë të kornizës, duke çuar në ndryshime më të gjera dhe institucionale. Siç u theksua më lart, në rastin e ushtrisë amerikane, zhvillimi veçanërisht në teknologjinë e helikopterëve nxiti ndryshime në doktrinën, organizimin dhe trajnimin e personelit me misionin e ri të tij.

---

[9] Kolonel Arben Dhuli, gazeta "Ushtria" 12 korrik 2024.

Dinamika e lidhjes në komponentin material është ajo ku evolucioni doktrinar formon strategjinë e përmirësimit të pajisjeve ushtarake në një forcë të caktuar apo institucion ushtarak. Si rezultat i ndryshimeve në këndvështrimin doktrinar mbi luftën, është arritur edhe integrimi i teknologjisë ushtarake, si: te tanket, avionët, artileria, teknologjia dhe komunikimi. Teknologjisë i është dhënë një vend parësor në doktrinat operacionale në luftën e re të epokës digjitale në moshën e Chat Gbt.

Më herët këndvështrimi doktrinar mbi luftën e mbështetur në "manovër" në ushtrinë amerikane evoluoi për të përzgjedhur blerjen e pajisjeve, megjithëse u prit me skepticizëm nga disa udhëheqës të ushtrisë së asaj kohe. Eisenhower[10] është një referencë e shkëlqyer edhe për këtë element. Ai komandoi një nga dy brigadat eksperimentale të tankeve në Fort Meade, Maryland, në vitet 1920. Duke shfaqur largpamësi operacionale për të ardhmen e luftës manovruese, Eisenhower besonte se tanket kishin potencial më të madh, për aplikimin e tyre në luftë, sesa thjesht mbështetja e këmbësorisë. Eisenhower dhe Patton[11] kundërshtuan doktrinën ekzistuese institucionale që e lidhte zhvillimin e tankeve vetëm me të qenit armë mbështetëse e këmbësorisë.

Kjo doktrinë kishte penguar përmirësimet e tankeve për sa i përket shpejtësisë së lëvizjes në fushën e luftimit ashtu edhe trashësisë së blindimit. Tanket kanë një rol të vlefshëm dhe më spektakolar, kështu që ata duhet të ishin më të shpejtë, që të sulmonin në befasi dhe të mbronin efektivët nga fuqia e zjarrit armik. Duke shfrytëzuar terrenin, ata mund të depërtojnë në pozicionet mbrojtëse të armikut dhe të shkaktojnë konfuzion, duke marrë vijën e parë të armikut, bëjnë të mundur avancim të këmbësorisë, por edhe përparime në pozicionet mbrojtëse. Eisenhower dhe Patton përfundimisht publikuan gjetjet e punës së tyre në revista profesionale, por u qortuan për sfidimin e doktrinës së manovrimit me qendër mbështetjen e këmbësorisë.

Një shembull tjetër se si ndryshimi doktrinar nxiti ndryshime në blerjen e materialeve është edhe përvoja e ushtrisë amerikane në Vietnam. Ushtrisë iu desh të përshtaste doktrinën dhe organizimin për të luftuar në mënyrë efektive në zonat bregdetare të Vietnamit, në jug të qytetit të njohur Saigon. Komanda Luftarake e Ushtrisë Amerikane zhvilloi një koncept për të adresuar sfidën e re duke përshtatur një brigadë të këmbësorisë në një forcë lumore të pajisur me varka dhe armë detare për të kryer operacione lumore të paparashikuar deri në atë kohë.

---

[10] https://www.airlant.usff.navy.mil/Organization/Aircraft-Carriers/USS-Dwight-D-Eisenhower-CVN-69/Namesake-Dwight-D-Eisenhower/

[11] https://www.nationalww2museum.org/war/articles/general-george-s-patton-jr-death

6. Lidershipi dhe arsimimi, faktorët bazë në përafrimin e njerëzve me sistemet, burimet dhe vizionin e FA-ve

Komponenti i DOTMLPF-P fokusohet në mënyrën se si FA-të edukojnë dhe zhvillojnë liderët e saj në të gjitha nivelet. Lidershipi dhe edukimi janë pjesë përbërëse e modernizimit të ushtrisë, sepse drejtuesit e saj janë përgjegjës si për funksionimin e përditshëm, ashtu edhe për transformimin afatgjatë të FARSH, në rastin tonë. Drejtuesit e lartë të forcave të armatosura ofrojnë drejtim, i cili përfshin përafrimin e njerëzve, sistemeve, burimeve dhe vizionin në nivel FA-je, për t'u fokusuar në aktivitetet e përditshme transformuese. Kolegji i Luftës së Ushtrisë Amerikane e përkufizon udhëheqjen strategjike si "procesin e përafrimit të njerëzve, sistemeve dhe burimeve, duke mundësuar një kulturë të përshtatshme dhe inovative të nevojshme, me qëllim për të fituar avantazh në mjedisin konkurrues".

Mënyra se si zgjidhen, arsimohen dhe punësohen liderët ushtarakë mbart implikime serioze për suksesin e misionit të FA-ve, si dhe për modernizimin institucional. Kjo është e dukshme në qasjet e të gjitha ushtrive të cilat e kanë zhvilluar atë në epokën e luftërave. Në përpjekjet për modernizim, FA-të lipset që sot krahas cilësisë në arsimin e oficerëve dhe nënoficerëve, me një fokus të veçantë duhet të trajtohet arsimimi teknik dhe teknologjik në fushën e AI. Ushtria profesionale e shekullit të 21-të do ketë nevojë gjithmonë për të promovuar edukimin teknik brenda korpusit të oficerëve dhe nënoficerëve. Ushtria profesioniste shqiptare si pjesë e NATO-s, do të drejtohet nga ushtarakët me shërbim afatgjatë, të kualifikuar qysh në fillim të karrierës së tre të cilët i janë nënshtruar një programi trajnimi të vazhdueshëm dhe të pandërprerë.

Përparimi i karrierës së nënoficerëve është gjithashtu shumë konkurrues në realitetin e sotëm. Duke besuar se e ardhmja e luftërave është ajo e parregullt, e cila zhvillohet kryesisht në nivelin taktik, roli i nënoficerit është rritur së tepërmi. Shembujt në arsimin e udhëheqësve në ushtrinë amerikane theksojnë rëndësinë jetike për modernizimin dhe efektivitetin e misionit me kalimin e viteve. Gjatë karrierës së tij, koloneli Xhorxh C. Marshall[12] zhvilloi reforma të thella arsimore të cilat e ndihmuan ushtrinë amerikane të rriste brezin e udhëheqësve luftarakë, që e drejtuan atë gjatë Luftës së Dytë Botërore.

---

[12] https://marshallcenteralbania.org/

Mandati i reformës Marshall në Shkollën e Këmbësorisë njihet si “reforma Benning”,[13] sepse ai zbatoi ndryshime në kurrikulën e shkollës, bazuar në një këndvështrim të qartë dhe të saktë mbi karakterin në zhvillim të luftës në dekadat pas viteve 1920. Ai parashikoi që luftërat e ardhshme do të ishin luftëra me manovrueshmëri dhe lëvizshmëri të shpejtë, të mbushura me pasiguri, që do të kërkonin liderë luftarakë që ishin vizionarë, përshtatës dhe krijues. Ai përshtati kurrikulën e shkollës për të nxitur kreativitet tek oficerët duke futur ushtrimet ushtarake që ata duhej të zgjidhnin në të njëjtin nivel me atë që kishte përjetuar në Luftën e Parë Botërore. Ai besonte në trajnimin e oficerëve për të marrë vendime në kohë dhe efektive me pak informacion dhe rrethana të pasigurta.

George Marshall tregoi interes të veçantë në menaxhimin e oficerëve për të siguruar që ushtria të kishte udhëheqjen më të aftë që i nevojitej për të luftuar dhe fituar. Sipas Benjamin Runkle[14], Marshall loboi në Kongres për një amendament që të tërhiqte shumë oficerë të vjetër në shërbim, intelekti dhe aftësia fizike e të cilëve ai gjykonte se ishin të duhurat në drejtimin e operacioneve luftarake. Marshall krijoi një bord prej gjashtë oficerësh në pension, të udhëhequr nga ish-shefi i shtabit të ushtrisë Malin Craig dhe i ngarkoi ata të rishikonin vlerësimet e efikasitetit të oficerëve më të vjetër. Në gjashtë muajt e parë të tij, paneli tërhoqi në shërbim aktiv nga pensioni 195 kapitenë, majorë, nënkolonelë dhe kolonelë. Në perspektivën e Forcave të Armatosura Shqiptare, gjykoj që duhet të ndiqet e njëjta procedurë me oficerë kryesisht me grada të larta, të dalë në rezervë apo që plotësojnë moshën për të dalë në rezervë, duke i thirrur dhe mbajtur në shërbim aktiv pikërisht për arsye të lidershipit dhe edukimit të tyre cilësor.

7. Personeli, si forca e gjallë më e rëndësishme e një force të armatosur

Burimet njerëzore drejtuese janë forca më e madhe e gjallë e ushtrisë. Burimet e duhura njerëzore janë të nevojshme për personelin dhe udhëheqjen e njësive luftarake dhe organizatave të tjera brenda një force të armatosur. Kjo e bën komponentin e personelit një element jetik të kornizës DOTMLPF-P. Në thelb, funksionimi i përditshëm i një institucioni ushtarak dhe modernizimi afatgjatë i tij, nuk mund të ndodhë pa ushtarakë të mirë dhe punonjës civilë të përkushtuar në radhët e tij. Ky kuptim i elementit të personelit në kornizën DOTMLPF-P çon në shqyrtimin e shqetësimeve të rekrutimit, përdorimit dhe mbajtjes së personelit ushtarak në një treg konkurrues pune.

Ushtria amerikane u përball me sfida të personelit që ishin problematike për t’i kapërcyer udhëheqësit e saj gjatë dy luftërave botërore. Gjenerali Marshall merrej me vështirësitë në rekrutimin dhe mbajtjen e personelit ushtarak, si kapitalin njerëzor për të mbështetur gatishmërinë dhe modernizimin e ushtrisë. Ai ishte këmbëngulës dhe i disiplinuar në përpjekjet e tij për të përgatitur ushtrinë për luftë, gjë që përkoi me marrjen e detyrës së tij si shef i shtabit të përgjithshëm në shtator 1939. Një nga hapat e para që ndërmori ishte rritja e burimeve njerëzore dhe pajisjeve të ushtrisë, ku përmes takimeve me presidentin dhe anëtarët e kongresit, ai prezantoi në mënyrë bindëse nevojat për përgatitjen e kohës së luftës. Departamenti i Luftës ofroi 3 miliardë dollarë, që e lejoi ushtrinë të blejë artikuj kritikë për një forcë prej dy milionë personel, si dhe të ndërtojë një bazë të industrisë ushtarake të aftë për të furnizuar një forcë totale me personel prej katër milionësh.

---

[13] https://www.facebook.com/events/mcginnis-wickham-hall-karker-st-fort-benning-ga-31905/ocs-graduation/1477812052489999/

[14] https://advanced.jhu.edu/directory/benjamin-runkle/

Cilësia e jetës është thelbësore për ruajtjen dhe rritjen e moralit të personelit, për të cilën Marshall promovoi edhe një sërë nismash të tjera të një institucioni ushtarak, p.sh., në trajnim. Ky ndryshim në marrjen e personelit lejoi që shërbimi të rekrutonte vetëm vullnetarë që ishin të gatshëm të shërbenin. Ky zhvillim bëri të nevojshme një ndryshim në qasjen e ushtrisë ndaj stërvitjes, pasi qasja ekzistuese e trajnimit, e quajtur Programi i Trajnimit të Ushtrisë (ATP), ishte e orientuar të trajnonte sasi masive të rekrutuarve, për urgjencën e paraqitur. ATP-ja tashmë me vullnetarizmin, kërkonte përshtatje me një qasje të re stërvitore që nuk ishte e fokusuar në trajnimin masiv të ushtarëve, brenda një kohe të shkurtër, por më tepër në trajnimin e sasive më të vogla të ushtarëve për një standard më të lartë të aftësive luftarake dhe fiziko psikologjike.

8. Objektet dhe infrastruktura ushtarake janë jetike për strehim, trajnim dhe gatishmërinë luftarake dhe logjistike

Ky element i kornizës DOTMLPF-P fokusohet në infrastrukturën që mbështet operacionet dhe aktivitetet e përditshme të FA si institucion. Ushtarët dhe jetesa e tyre në garnizone ka prioritet, i cili kërkon ndërtimin e objekteve të përshtatshme në strehimin, trajnimin, arsimin, gatishmërinë logjistike dhe veprimtarinë e përditshme. Është e pamundur të modernizohet FA pa objektet e duhura, gjë që e bën komponentin infrastrukturor, kritik dhe shumë të rëndësishëm për vendin e tij në kuadrin DOTMLPF-P.

Ushtria amerikane shfrytëzoi objektet e saj të mëparshme stërvitore për të zhvilluar ndoshta fushatën më të madhe stërvitore të kohës që u quajtën “Manovrat e Luizianës” të vitit 1941. Ashtu si shumica e stërvitjeve ushtarake të këtij lloji, Manovrat e Luizianës ndihmuan në identifikimin e fushave të përmirësimit të nevojshëm për ushtrinë, si motorizimi por nxorën në pah edhe atributet e performancës dhe potencialin e ardhshëm të drejtuesve të një brezi në rritje oficerësh. Një shembull i këtij potenciali ishte kolonel Eisenhower[15] me detyrën e Shefit të Shtabit gjatë Manovrave të Luizianës 1941. Ai shkruan se tenda e tij u bë një vend ku njerëzit vinin për t'i besuar shqetësimet e tyre. Kjo ndërthurje e lidershipit dhe aftësive ndërpersonale do ta ndihmonte më vonë Eisenhower-in të menaxhonte me sukses marrëdhëniet e punës dhe personalitetet komplekse të vartësve të tij si Komandanti Suprem i Aleatëve në Luftën e Dytë Botërore.

---

[15] https://millercenter.org/president/eisenhower

Një shembull për t'u analizuar është "Yuma Proving Ground"[16], e cila është qendra kryesore e testimit të ushtrisë. Ky instalim ka rrezen më të madhe të artilerisë tokësore, ku ushtria bën testime qitje artilerie. Që nga viti 2020, Ushtria amerikane ka përdorur laboratorët e saj superiorë në bashkëpunim me objektet kryesore të testimit në Yuma Proving Ground, për të kryer një fushatë mësimi dhe eksperimentimi të quajtur "Project Convergence"[17]. Project Convergence është forca e përbashkët (JF) që eksperimenton me shpejtësinë, rrezen dhe dominimin e vendimeve, për të arritur përputhje dhe informuar mbi konceptin e luftimit të përbashkët dhe komandën dhe kontrollin (C2) e luftës në shumë domene. Ajo aktualisht përdor një sërë angazhimesh të përbashkëta, për të integruar inteligjencën artificiale, robotikën dhe armëve autonome, për të përmirësuar fushën e betejës dhe përshpejtuar afatin kohor të vendimmarrjes.

Projekti është infrastrukturë kritike jo vetëm për faktin e modernizimit të vazhdueshëm të Ushtrisë, por edhe për forcën e SHBA-së dhe aleatëve të saj. Suksesi i projektit varet nga zhvillimi, testimi dhe pajisjet e eksperimentimit të institucionit. Kjo nënvizon edhe një herë rëndësinë kritike të elementit infrastrukturor të kornizës DOTMLPF-P për transformimin dhe modernizimin progresiv të FA. Sipas Komandës së Materialeve të Ushtrisë, OIB[18] përbëhet nga objektet teknike dhe një fuqi punëtore e kualifikuar, që ndihmojnë ushtrinë të modernizojë dhe të gjenerojë gatishmëri operacionale përmes mirëmbajtjes dhe riparimit. Ndër këto objekte është "Anniston Army Depot"[19], e cila ofron ekspertizë për automjete të rënda luftarake si dhe armët e kalibrit të vogël.

9. Politika si autoriteti vendimmarrës dhe miratues i planeve të modernizimit

Politika e ka autoritetin dhe mandatin institucional për të miratuar, financuar dhe nxitur modernizimin e ushtrisë. Politika ka rol kyç për të evoluar dhe menaxhuar komponentët e tjerë të kornizës DOTMLPF-P. Ky rol meriton një vend parësor për politikën në kornizë si dhe nënvizon rëndësinë e tij për modernizimin e ushtrisë. Politikat mund të pengojnë ose nxisin një institucion ushtarak që e percepton dhe ndërvepron me ambiciet për përmirësim. Për shembull, *Army Acquisition Policy*[20] " drejton kërkimin, zhvillimin, blerjen dhe menaxhimin e ciklit të plotë jetësor të pajisjeve të FA për të përmbushur kërkesat e miratuara në aftësitë luftarake. Kjo rregullore për arsye të politikës që përfshin thelbin e saj, ka përparësi ndaj rregulloreve të tjera të ushtrisë në lidhje me menaxhimin e programeve të blerjes së FA.

---

[16] https://home.army.mil/yuma

[17] https://www.defense.gov/Spotlights/Project-Convergence-Capstone-4/

[18] https://www.army.mil/standto/archive/2022/03/25/

[19] https://anad.army.mil/

Ndryshimet në politikën e blerjes së FA e kanë ndihmuar atë të modernizohet duke i përmirësuar proceset e blerjes së materialeve. Edicioni 2018 i AR 70-1[21] përfshin iniciativa të reja të blerjeve të cilat përmirësojnë efikasitetin, gatishmërinë, testimin, vlerësimin, integrimin e shkencës dhe teknologjisë në zhvillimin e aftësive dhe fokus më të madh në sigurinë kibernetike. Ndryshimet nga kongresi në politikën ushtarake të SHBA e ndihmuan ushtrinë të përgatitej për të fituar Luftën e Dytë Botërore. Këto ndryshime politikash ndodhën falë përpjekjeve lobuese të drejtuesve të gjeneralit Marshall. Për shkak të këmbënguljes së Marshall, "Shtetet e Bashkuara zbatuan politika të reja për të zhvilluar fuqinë njerëzore, për të ngritur industrinë, për të rritur shpenzimet e mbrojtjes, për të rikthyer fokusin te stërvitjet dhe gatishmëria, si dhe për të zhvilluar plane mobilizimi që do të shërbenin si bazë për përgatitjet e SHBA për luftë.

Marshall inicioi ndryshime politikash që e reformuan burokracinë e ushtrisë, përmirësuan vendimmarrjen e drejtuesve të lartë, pasi kur ai mori detyrën si Shefi i Shtabit të Ushtrisë, vuri re se shtabi i përgjithshëm i Departamentit, ishte bërë joefikas dhe jo operativ. Shumë oficerë kishin akses të drejtpërdrejtë te Shefi i Shtabit, ndërsa krerët e agjencive autonome ruanin privilegjet dhe humbnin kohë dhe energji në mosmarrëveshje të vogla· Pas sulmit japonez në Pearl Harbor, Marshall vërejti: "U deshën ditë të tëra për të marrë një letër vlerësuese nga departamenti i luftës, pasi nuk binin dakord të gjithë me draftin. Marshall ricaktoi një oficer të përgjithshëm, Joseph McNarney si ndërlidhës i cili zvogëloi numrin e individëve me akses të drejtpërdrejtë tek ai, nga gjashtëdhjetë në gjashtë dhe tre komanda të reja, Tokësore, Ajrore dhe Forcat mbështetëse të drejtuar nga gjeneralët Lesley McNair, Hap Arnold dhe Brehon Somervell. Si rezultat i këtij ndryshimi, ushtria tani është në gjendje të aplikojë talentin nga tërësia e kapitalit të saj njerëzor në armët luftarake, e pakufizuar nga normat e vjetra gjinore.

Ky është një shembull i shkëlqyer edhe për FARSH i cili tregon se si ndryshimet e politikave formësojnë mënyrën se si një institucion ushtarak percepton dhe ndërvepron me mundësitë e reja dhe të vazhdueshme për përmirësim.

---

[20] https://www.dami.army.pentagon.mil/site/ARTPC/docs/ar70_1.pdf

[21] https://dml.armywarcollege.edu/wp-content/uploads/2024/01/AR-70-1-Adaptive-Acquisition-Framework-2023.pdf

Gjenerali James McConville[22] në 2020 pohoi se modernizimi i Ushtrisë duhet të vazhdojë: “Ne duhet të modernizojmë tani. Nuk ka të bëjë me luftën e fundit, por më mirë. Bëhet fjalë për të fituar luftën e radhës. Për ta bërë këtë, ne duhet të transformohemi.”

Përfundime

- Modernizimi i FA nxit zhvillimin doktrinar përmes inovacionit teknologjik. Përpjekjet për modernizimin e ushtrisë do të vazhdojnë pa ndërprerje dhe gjithmonë gjeneratave të reja të drejtuesve do iu nevojitet përvoja e paraardhësve.
- Ky punim ndihmon brezat e profesionistëve që po hyjnë në strukturat e modernizimit të ushtrisë, për t’i krijuar atyre një kornizë praktike ndihmuese, si dhe për të vijuar përpjekjet e vazhdueshme dhe pandërprera të këtij procesi.
- Analizat e mëparshme të rolit të secilit element të DOTMLPF-P, të plotësuara me shembuj të reformave aktuale ushtarake të epokës digjitale, tregojnë se si modernizimi evoluon nga luftërat e shkuara, konfliktet në zhvillim dhe do të vazhdojë në të ardhmen.
- Fokusimi në një element ose komponent të DOTMLPF-P dhe shpërfillja e të tjerëve nuk këshillohet, sepse mund të shkaktojë një çekuilibër cenues për misionin, sepse elementët e kornizës janë të ndërlidhur dhe plotësues të njëri-tjetrit.
- Modernizimi i FARSH duhet të jetë zhvillimi progresiv i të gjitha elementeve kritike me anë të të cilave institucioni përcakton, ndërton dhe operon nga konteksti aktual, duke parashikuar për transformimin modernizues të ushtrisë së të ardhmes.

Bibliografia

1. “Military Doctrine” RAND, accessed 3 January 2022, http://www.rand.org/topics/military-doctrine.html.
2. Corum, *The Roots of Blitzkrieg*, 70.
3. Eisenhower, *At Ease*, 236.
4. Department of the Army, *Yuma Proving Ground*, accessed 3 August 2022.
5. Army Futures Command, “Project Convergence,” accessed 23 January 2023.

---

[22] https://www.dvidshub.net/video/769441/general-james-c-mcconville-2020-ausa-now-conference

6. U.S. Army Materiel Command, “Army Organic Industrial Base Modernization Implementation Plan,” *Stand-To!* 25 March 2022.
7. Department of the Army, Army Regulation (AR) 70-1: *Research Development and Acquisition: Army Acquisition Policy* (Washington, DC: U.S. Government Printing Office, 10 August 2018).
8. Sean M. Zeigler et al., *The Evolution of U.S. Military Policy from the Constitution to the Present, Volume II: The Formative Years for U.S. Military Policy, 1898–1940* (Santa Monica, CA: RAND, 2019), 103.
9. Unger, *George Marshall*, 159.
10. Forrest C. Pogue, *George C. Marshall: Ordeal and Hope, 1939 1942* (New York: Viking Press, 1966), 293, as quoted in Unger, George Marshall, 159.
11. Unger, *George Marshall*, 160.
12. General James McConville in Rick Maze, “Urgent Push: McConville: ‘We Must Modernize Now,’” *Army Magazine*, 14 January 2021.

Rëndësia e dronëve në zbulimin dhe shuarjen e zjarreve

Kolonel Msc. David RROKU
Zëvendësdrejtor i IKSHU

Trajtesë e shkurtuar.

Ky punim do të trajtojë krijimin dhe vlerësimin e një droni zjarrfikës për përgjigje emergjente. Droni ka për qëllim të mbështesë zjarrfikësit në kushte të rrezikshme, veçanërisht gjatë zjarreve në pyje kur afrimi i njerëzve mund të jetë i vështirë dhe i rrezikshëm. Droni ka një kamerë termike (një kamerë me rezolucion të lartë), një rezervuar uji në bord për shuarjen e flakëve me ujë. Për dizajnimin dhe zhvillimin e dronit janë përdorur metodat e avancuara të printimit 3D dhe simulimet kompjuterike. Aftësitë e dronit janë vënë në provë në një mjedis të sigurt dhe rezultatet treguan se sa i mirë është ai për luftimin e zjarreve. Shkrimi vazhdon me një diskutim të përdorimit të mundshëm të dronëve zjarrfikës në menaxhimin e fatkeqësive dhe çështjet që duhet të zgjidhen për të mundësuar përdorimin e tij të sigurt dhe efikas në situata praktike. Droni u krijua kryesisht për të luftuar zjarret; është i pajisur me spërkatës me gaz, uji dhe fikse. Gama e tij e funksionimit e lejon atë të shuajë me sukses flakët në struktura të mëdha dhe të arrijë lartësi të mëdha. Në mjedisin eksperimental, një zonë me bar u dogj qëllimisht dhe ritmi i përhapjes dhe intensiteti i zjarrit u menaxhuan duke ndryshuar shpejtësinë e erës dhe ngarkesën e karburantit. Dronët e përdorur për këtë qëllim kanë kamera infra të kuqe si dhe sensorë tymi. Efektiviteti i dronëve u vlerësua në bazë të prirjes së tyre për të dalluar dhe shuar flakët, si dhe në atë se sa shpejt dhe manovrueshëm mund të lëviznin nëpër rajonin e djegur.

Fjalë kyçe: Dronë, zjarrfikës, pajisje zjarrfikëse, menaxhimi i fatkeqësive.

Hyrje

Ndërsa teknologjia zhvillohet, po krijohen qasje të reja dhe kreative për të trajtuar çështjet dhe për të përmirësuar sigurinënë një sërë sektorësh. Beteja kundër zjarreve është një fushë ku teknologjia ka potencialin të ketë një ndikim të madh. Çdo pajisje që do ta bënte shuarjen e zjarrit më pa rrezik dhe produktive për zjarrfikësit do të ishte e paçmuar.[1]

Luftimi i flakëve është një punë e rrezikshme dhe e vështirë. Përdorimi i dronëve është një teknikë inovative që po hulumtohet për shuarjen e zjarrit. Në disa përdorime, duke përfshirë fotografimin nga ajri, shërbimet e dorëzimit, madje edhe operacionet e kërkimit dhe shpëtimit, dronët tashmë janë dëshmuar shumë të dobishëm. Sidoqoftë, përdorimi i dronëve në luftimin e zjarreve është një përdorim shumë i ri dhe i paprovuar. Ndërsa ideja e dronëve të shuarjes së zjarrit është ende në fazën e saj eksperimentale, ka avantazhe të mëdha potenciale. Dronët janë të aftë të pajisen me kamera dhe sensorë që mund të lokalizojnë me shpejtësi dhe saktësi pikat e nxehta dhe vendndodhjet e tjera të mundshme të problemeve. Ato mund të përdoren gjithashtu për të transportuar materiale zjarrfikëse si uji, shkumë, apo edhe kimikate që rezistojnë zjarrin në vendin e zjarrit, të cilat mund të ndihmojnë në shuarjen e flakëve më shpejt dhe me efikasitet[2].

Përdorimi i dronëve në luftimin e zjarreve mund të kontribuojë gjithashtu në sigurinë e zjarrfikësve. Duke dhënë imazhe nga lart të zjarrit dhe vendndodhjeve aty pranë, dronët mund të ndihmojnë zjarrfikësit të zbulojnë kërcënimet e mundshme dhe t'i shmangin ato. Për më tepër, zjarrfikësit në terren mund të marrin informacion në kohë reale nga dronët, duke u mundësuar atyre të marrin vendime më të informuara se ku për të përqendruar përpjekjet e tyre. Pavarësisht nga avantazhet e mundshme të dronëve zjarrfikës, disa çështje ende duhet të zgjidhen, p.sh., dronët duhet të jenë në gjendje të funksionojnë në situata me temperaturë të lartë dhe të durojnë ekspozimin ndaj zjarreve dhe tymit[3].

Përveç kësaj, ata duhet të jenë në gjendje të manovrojnë nëpër mjedise sfiduese si ndërtesat ose pyjet duke shmangur rreziqet. Ka konsiderata shtesë ligjore dhe rregullatore që duhen adresuar. Aktualisht ka kufizime se ku dhe si mund të përdoren dronët në shuarjen e zjarrit, dhe përdorimi i tyre është shumë i rregulluar[4]. Por, ndërsa teknologjia vazhdon të rritet dhe të maturohet, parashikohet që këto ligje të bëhen më fleksibël dhe të lejojnë më shumë përdorim të dronëve në operacionet e shuarjes së zjarrit. Në këtë shkrim, do të studiojmë zhvillimi i dronëve zjarrfikës dhe përdorimi i mundshëm i tyre në mjediset reale të shuarjes së zjarrit.

---

[1] K. Valavanis, G. Vachtsevanos, "Aplikacionet UAV", Në Manualine Mjeteve Ajrore pa pilot. Valavanis Springer: Berlin, Gjermani,vëll. 3, fq. 2639–2641, 2015

[2] E. Lygouras, A. Gasteratos, K. Tarchanidis, Mitropoulos, A. ROLFER: "Një sistem mbështetës i shpëtimit ajror plotësisht autonom" Mikroprocesi. Microsyst, vëll. 61, fq. 32–42, 2018

[3] J. Tomotani, "Përdorimi i mjeteve ajrore pa pilot në operacionet ekërkimit", J. Geek Stud, vëll. 2, f. 41–53, 2015

Më poshtë do të trajtojmë problemet teknologjike që duhet të zgjidhen, si dhe konsideratat ligjore dhe rregullatore që duhet të merren parasysh. Sigurisht që do të shikojmë gjithashtu llojet e ndryshme të dronëve zjarrfikës që janë aktualisht në treg, së bashku me avantazhet dhe dizavantazhet e secilit prej tyre[5]. Gjatë gjithë këtij shkrimi, do të jap përditësime mbi zbulimet më të reja në teknologjinë e dronëve të shuarjes së zjarrit dhe do të ndajmë pikëpamjet e profesionistëve në këtë industri. Objektivi është të ofrojmë një pasqyrë të plotë të avantazheve të mundshme të dronëve të zjarrfikësve, si dhe vështirësive që duhet të kapërcehen që kjo teknologji të bëhet realitet.

Ekologjia dhe jetët e njerëzve janë të rrezikuar seriozisht nga zjarret në pyje[6]. Agjencia Kombëtare e Mbrojtjes Civile vlerëson se kohët e fundit janë shtuar zjarret në të gjithë territorin e Republikës së Shqipërisë dhe janë djegur me mijëra hektar pyje dhe kullota, si dhe janë rrezikuar shumë shtëpi banimi. Zjarret në pyje po bëhen gjithnjë e më të rënda dhe më të shpeshta, gjë që thekson nevojën për zgjidhje kreative për ndalimin e këtyre katastrofave. Për të rritur efikasitetin dhe sigurinë e operacioneve të shuarjes së zjarrit, përdorimi i dronëve është shfaqur si një alternativë e mundshme[7]. Zjarrfikësit mund të analizojnë situatën, të hartojnë një plan veprimi dhe të ndërmarrin veprime të menjëhershme me përdorimin e dronëve që mund të ofrojnë monitorim dhe mbikëqyrje në kohë reale të zjarrit. Në këtë botim eksperimental, ne përshkruajmë krijimin dhe vlerësimin e një droni zjarrfikës që synon të mbështesë zjarrfikësit në rrethana të rrezikshme. Droni ka një kamerë termike, një rezervuar uji në bord për shuarjen e flakëve me ujë dhe një kamerë me rezolucion të lartë.

1. Mënyra e kërkimit

Në luftën kundër zjarreve dhe zjarreve të tjera në shkallë të gjerë, dronët e shuarjes së zjarrit janë një mjet vendimtar. Këta dronë mund t'i ofrojnë personelit zjarrfikës informacione dhe ndihmë jetike, duke i mundësuar atyre të shuajnë flakët me sukses dhe më të sigurt. Një nga avantazhet kryesore të dronëve zjarrfikës është aftësia e tyre për të dhënë të dhëna dhe fotografi në kohë reale nga ajri[8]. Ky informacion mund të ndihmojë për të kuptuar më mirë madhësinë dhe shtrirjen e zjarrit, vendndodhjen e pikave të nxehta dhe vlerësimin e rreziqeve të mundshme ose vështirësitë që lidhen me shuarjen e zjarrit. Dronët mund të përdoren gjithashtu për të ofruar furnizime, të tilla si uji ose parandalues zjarri, në zona që janë të vështira ose të rrezikshme për t'u arritur nga forcat zjarrfikëse[9]. Krijimi dhe përdorimi i dronëve zjarrfikës pengohet nga disa boshllëqe kërkimore. Zhvillimi i teknologjive më të sofistikuara të imazhit dhe sensorëve që mund të ofrojnë informacion më të saktë rreth zjarreve është një fushë thelbësore studimi. Kjo përfshin krijimin e kamerave termike që mund të identifikojnë zonat e nxehta dhe aplikimin e algoritmeve të mësimit të makinerive për të vlerësuar të dhënat e zjarrit në kohë reale[10].

---

[4] E. Lygouras, A. Gasteratos, K. Tarchanidis, Mitropoulos, A. ROLFER: "Një sistem mbështetës i shpëtimit ajror plotësishtautonom," Mikroprocesi. Microsyst, vëll. 61, fq. 32–42, 2018

[5] A. Carrio, C. Sampedro, A. Rodriguez-Ramos, P. Campoy, "Një përmbledhje e metodave dhe aplikimeve të tëmësuarit të thellë për mjetet ajrore pa pilot", J. Sens, f. 1–13,2015

[6] E. Petritoli, F. Leccese, L. Ciani, "Analiza e besueshmërisë dhe e mirëmbajtjes së mjeteve ajrore pa pilot", Sensorët, vëll. 18, f. 56-71, 2018.

[7] S. Saponara, "Sistemet e ndjeshmërisë dhe lidhjes për drejtimin e asistuar dhe autonome dhe automjetet pa pilot", Sensors, vëll.18, f. 19-29, 2018.

Një fushë tjetër kryesore e studimit është krijimi i teknikave më efektive dhe efikase të shpërndarjes për furnizimet e zjarrfikësve. Kjo përfshin krijimin e dronëve që mund të mbartin ngarkesa më të mëdha dhe vendosjen e materialeve dhe teknologjisë së re për të rritur efikasitetin e rezistentëve ndaj zjarrit dhe produkteve të tjera zjarrfikëse[11]. Së fundmi, ekziston nevoja për studime shtesë për sigurinë dhe besueshmërinë e dronëve zjarrfikës. Kjo përfshin krijimin e sistemeve të besueshme të komunikimit dhe kontrollit për të garantuar që dronët mund të përdoren në mënyrë të sigurt në mjedise me rrezik të lartë, si dhe krijimin e masave të sigurta për të ndaluar përplasjen me njëri-tjetrin ose mosfunksionimin e dronëve gjatë aktiviteteve të shuarjes së zjarrit[12].

2. Qëllimi i përdorimit

Objektivi i ri i dronëve zjarrfikës është të sigurojë një mjet më të shpejtë dhe më efektiv për shuarjen e flakëve. Zjarrfikësit mund të bëjnë gjykime më të mira se si të luftojnë zjarrin me përdorimin e dronëve, të cilët mund të ofrojnë informacion në kohë reale për vendndodhjen dhe intensiteti i zjarrit. Dronët mund të përdoren potencialisht për t'u shërbyer zjarrfikësve duke transportuar mjete dhe furnizime si ujë ose aparate zjarri. Përdorimi i dronëve zjarrfikës për të pakësuar rrezikun për zjarrfikësit është një tjetër përdorim në zhvillim e tyre. Dronët mund të arrijnë vende që janë shumë të rrezikshme për afrimin e zjarrfikësve, duke përfshirë strukturat e djegura ose rajonet me shumë tym[13].

---

[8] A. Adam, M. Elmaleeh, Mahmoud, D. "Një algoritëm i bazuar në rrjetin nervor inteligjent për kontrollin e uljes së mjetit ajror autonome pa pilot".

[9] K. Vijayakumar, S. Suchitra dhe P. Swathi Shri, "Një auditim i sigurt i ruajtjes së reve me a. kontraktimi empirik i përditësimeve kryesore", Int. J. Sistemet Inteligjente të bazuara në arsyetim, vëll. 11, nr. 2,2019.

[10] Hugo Rodrigue, Seunghyun Cho, Min-Woo Han, Binayak Bhandari, Jae-Eul Shim & Sung-HooAhn ., Effect of twist morphing wing segment on the aerodynamic performance of UAV., Journal of Mechanical Science and Technology., 2016

[11] Fu-Hsuan Wen, Fu-Yuen Hsiao, and Jaw-Kuen Shiau, Analysis and Management of Motor Failures of Hexacopter in Hover, Department of Aerospace Engineering,2021

[12] Huy X. Pham; Hung M. La; David Feil-Seifer; Matthew Deans, A distributed control framework for a team of unmanned aerial vehicles for dynamic wildfire tracking, 2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)., 2017.

Dronët e përdorur për shuarjen e zjarrit përdoren për të zbuluar, ndaluar përhapjen e flakëve si dhe shuarjen e tyre.

Figura nr. 1. Kontrolli i dronëve zjarrfikës.

Përdorimi i dronëve për të monitoruar mjedisin për zjarre të mundshme është një tjetër përdorim inovativ për pajisjet e zjarrfikësve.

Në dronë mund të instalohen sensorë që mund të identifikojnë ndryshimet e temperaturës, lagështisë dhe variablave të tjerë mjedisorë që mund të rrisin rrezikun e zjarreve. Zjarrfikësit mund ta përdorin këtë informacion për t'u informuar për rreziqet e mundshme të zjarrit, në mënyrë që të marrin masa paraprake përpara se të fillojë një tillë. Për të shuar në mënyrë efektive zjarret, dronët zjarrfikës duhet të kapërcejnë disa pengesa[14].

---

[13] Hugo Rodrigue, Seunghyun Cho, Min-Woo Han, Binayak Bhandari, Jae-Eul Shim & Sung-HooAhn ., Effect of twist morphing wing segment on the aerodynamic performance of UAV., Journal of Mechanical Science and Technology., 2016.

[14] WildfireCauses. Fire and Aviation Management, National Park Service U.S Department of InteriorAvailable online: cfm (accessed on 6 December 2017)

Disa nga sfidat kryesore përfshijnë:

- Dronët duhet të jenë në gjendje të lundrojnë në një mjedis të ngjeshur dhe dinamik, duke shmangur njëkohësisht pengesat dhe duke mbajtur fluturim të qëndrueshëm. Në rrethana me erë, të cilat mund të ndikojnë në stabilitetin e dronit dhe të krijojnë turbulenca, kjo mund të jetë shumë sfiduese. Dronët e përdorur në shuarjen e zjarrit duhet të jenë në gjendje të transportojnë një ngarkesë të madhe, si uji ose aparate të tjerë zjarri. Kjo kërkon një motor dhe bateri të fortë, të cilat mund të rrisin peshën e dronit dhe të shkurtojnë kohën e fluturimit.
- Koha e kufizuar e fluturimit: Dronët kanë një kohë të kufizuar fluturimi për shkak të jetëgjatësisë së baterisë, e cila mund të jetë problematike për shuarjen e flakëve që kërkojnë shumë kohë për t'u shuar. Si rezultat, dronët mund të kenë nevojë të përdoren përveç mjeteve të tjera të zjarrfikësve si ekuipazhet tokësore ose helikopterët.
- Dronët duhet të jenë në gjendje t'i rezistojnë si nxehtësisë së madhe ashtu edhe flakës së zjarrit ndërsa vazhdojnë të funksionojnë. Kjo mund të arrihet duke përdorur materiale rezistente ndaj zjarrit dhe sisteme ftohjeje, por këto i shtojnë peshë dhe kompleksitet shtesë dronit [15].
- Dronët e zjarrfikës duhet të jenë në gjendje të koordinojnë lëvizjet dhe veprimet e tyre me burime të tjera, si dhe me ekuipazhet me bazë në tokë, për të siguruar shuarjen efektive të zjarrit. Për këtë nevojiten sisteme dhe protokolle të forta komunikimi, si dhe operatorë të aftë që mund ta kontrollojnë atë në një mjedis dinamik[16].

3. Projektimi dhe zhvillimi

Dizajni dhe zhvillimi i dronit është kryer duke përdorur teknika të avancuara të printimit 3D dhe simulime softuerike. Trupi i dronit është bërë nga materiale të lehta dhe të qëndrueshme, duke e bërë atë të aftë të përballojë kushtet ekstreme që hasen në shuarjen e zjarrit. Rotorët dhe sistemi i shtytjes së dronit u optimizuan për të siguruar stabilitet dhe manovrim, duke e lejuar atë të fluturojë nëpër mjedise të ngushta dhe komplekse. Kamera e dronit dhe teknologjia e imazhit termik u zgjodhën me kujdes për të ofruar imazhe me rezolucion të lartë dhe të dhëna të temperaturës në kohë reale të zjarrit[17].

---

[15] Remington, R.; Cordero, R.; March, L.; Villanueva, D. Multi-Purpose Aerial Drone for Bridge Inspection and Fire Extinguishing. Unpublished Thesis, Florida International University, Miami, FL, USA, 2016. [20] Marchant, W.; and Tosunoglu, S. Rethinking Wildfire Suppression with Swarm Robotics. In Proceedings of the 29th Florida Conference on Recent Advances in Robotics, FCRAR'16, Miami, FL, USA, 12–13 May 2016.

[16] Key Findings from the 2017 Verisk Wildfire Risk Analysis, 2 December 2017.

[17] Death and destruction in the Philippines," IFSEC PHILIPPINES, 2019.

Rezervuari i ujit në bord është projektuar për të siguruar furnizim të mjaftueshëm me ujë për shuarjen e zjarrit. Kapaciteti i rezervuarit të ujit u optimizua për të balancuar peshën e dronit dhe kohën e fluturimit, duke siguruar që ai të mund të funksionojë me efikasitet për një periudhë të gjatë. Depozita e ujit është e pajisur me një mekanizëm spërkatës që mund të kontrollohet nga distanca për të rregulluar rrjedhën dhe drejtimin e ujit. Droni i propozuar zjarrfikës është projektuar për të operuar në një gamë të gjerë mjedisesh, duke përfshirë zonat urbane, rurale dhe industriale. Droni ka një konfigurim me katër kopter, i cili siguron stabilitet dhe manovrim në ajër.

Korniza e dronit është bërë nga pesha e lehtë, e lartë materialet e forta, të tilla si fibra karboni, për të zvogëluar peshën dhe për të rritur kapacitetin e ngarkesës[18]. Dronët zjarrfikës janë një teknologji emergjente që po zhvillohet për të ndihmuar në menaxhimin dhe luftimin e zjarreve. Më poshtë janë të renditura disa tipe të dronëve zjarrfikës që janë në zhvillim ose që janë përdorur në mënyrë eksperimentale:

- **Dronët për monitorim dhe vlerësim:**

Dronë me kamera termike: Këta dronë janë të pajisur me kamera termike për të identifikuar burimet e nxehtësisë dhe për të vlerësuar shpërndarjen e zjarrit në terren. Ata ofrojnë një pamje të qartë të situatës dhe ndihmojnë ekipet e emergjencës të planifikojnë strategjitë e reagimit.

Dronë me sensorë ambientalë: Sensorët për temperaturën, lagështinë dhe gazrat e dëmshëm ndihmojnë në mbledhjen e të dhënave të detajuara për kushtet e zjarrit dhe për të ndihmuar në parashikimin e përhapjes së tij.

- **Dronët për dërgimin e lëngjeve:**

Dronë me rezervuarë të përdorshëm: Këta dronë janë të pajisur me rezervuarë për lëngje zjarrfikës. Ata mund të transportojnë dhe shpërndajnë materiale për të ndihmuar në kontrollimin e zjarrit në zona të vështira për t'u arritur.

***Dronë me sisteme të shpërndarjes së shpejtë*:** Dronë të tillë përdorin mekanizma të sofistikuar për të shpërndarë substanca të veçanta në zona të vogla dhe të përcaktuara me saktësi.

- **Dronët për dërgimin e pajisjeve të shpëtimit:**

Dronë me kapacitet për dërgimin e pajisjeve të shpëtimit: Këta dronë mund të dërgojnë pajisje të rëndësishme si kit të ndihmës së parë, radio-komunikimi ose rrethim mbrojtës në zona të izoluara ku ekipet e emergjencës nuk mund të arrijnë menjëherë.

---

[18] Marchant, W.; Tosunoglu, S. Rethinking Wildfire Suppression with Swarm Robotics. In Proceedings of the 29th Florida Conference on Recent Advances in Robotics, FCRAR'16, Miami, FL, USA, 12–13 May 2016.

Dronë me mënyra të rrugës së sigurt: Ata mund të përdorin teknologji për të naviguar në mënyrë të sigurt dhe për të shmangur pengesat që ndodhin gjatë operacioneve në kushte të vështira.

- **Dronët për parashikimin e shpërndarjes së zjarrit:**

Dronë me algoritme për analizën e të dhënave: Këta dronë përdorin algoritme dhe modele për të analizuar të dhënat dhe për të parashikuar shpërndarjen e zjarrit në bazë të kushteve të motit, terrenit dhe intensitetit të zjarrit.

Dronë për simulime dhe testime: Dronë të tillë mund të përdoren për të simuluar dhe testuar skenarë të ndryshëm të shpërndarjes së zjarrit për të përgatitur strategji më të efektshme për reagim.

- **Dronët për komunikimin dhe koordinimin:**

Dronë komunikimi: Këta dronë ofrojnë lidhje të qëndrueshme dhe të sigurt për komunikim ndërmjet ekipeve të emergjencës dhe për të ndihmuar në koordinimin e operacioneve gjatë situatave të krizës.

Dronë me sisteme të ndihmës për navigimin: Ata ndihmojnë në koordinimin e ekipeve të shpëtimit dhe për të siguruar që ndihma të arrijë në mënyrë të sigurt në zonat e prekura nga zjarri.

Çdo lloj droni ka përdorime dhe avantazhe të ndryshme dhe përzgjedhja e llojit të duhur do të varet nga nevojat specifike të misionit dhe nga kushtet në terren. Në përgjithësi, dronët zjarrfikës përfaqësojnë një hap të rëndësishëm përpara në teknologjinë e menaxhimit të emergjencave dhe mund të ndihmojnë në shpëtimin e jetëve dhe mbrojtjen e pasurive.

4. Vlerësimi i aftësisë së dronit për të fluturuar në kushte të vështira

Aftësia e dronëve zjarrfikës për të lundruar në kushte të vështira do të kërkonte një sërë testesh dhe vlerësimesh për të përcaktuar efektivitetin e tij[19]. Këtu janë disa faktorë që mund të merren parasysh, duke vlerësuar aftësinë fluturuese të dronit:

- **Shmangia e pengesave:** Droni duhet të jetë në gjendje të zbulojë dhe shmangë pengesat si pemët, ndërtesat dhe linjat e energjisë elektrike gjatë fluturimit në kushte të vështira.
- **Saktësia GPS:** Sistemi GPS i dronit duhet të jetë mjaft i saktë për të lundruar në zona me mbulim të dobët GPS ose ndërhyrje.
- **Kontrolli i lartësisë:** Droni duhet të jetë në gjendje të mbajë një lartësi të qëndrueshme në kushtet e ndryshimit të motit, duke përfshirë erërat e forta, rrëmbimet dhe turbulencat.

---

[19] G. Hovland dhe M. Ottestad, "Optimizimi i dizajnit të UAV me shumë kopter", në Konferencën e 10-të Ndërkombëtare mbi Sistemet dhe Aplikacionet Mekatronike dhe të Embedded (MESA), Senigallia, Itali, 2014.

- **Stabiliteti i fluturimit:** Droni duhet të jetë në gjendje të fluturojë në mënyrë të qëndrueshme në kushte të vështira, duke përfshirë erërat e kundërta, turbulencat.
- **Navigimi vizual:** Droni duhet të jetë në gjendje të përdorë shenja vizuale për të fluturuar në zonat ku mbulimi me GPS është i dobët, si në zona të dendura urbane ose pyje.
- **Përgjigja e urgjencës:** Droni duhet të jetë në gjendje t'i përgjigjet shpejt situatave emergjente, të tilla si zbulimi i zjarreve dhe sigurimi i të dhënave në kohë reale për zjarrfikësit në terren[20].
- **Jetëgjatësia e baterisë:** Droni duhet të jetë në gjendje të ruajë aftësinë e tij lundruese për një periudhë të gjatë, veçanërisht gjatë operacioneve të zgjatura të shuarjes së zjarrit.

5. Kapaciteti i ngarkesës

Kapaciteti i ngarkesës është një faktor kritik për t'u marrë parasysh kur bëhet fjalë për dronët e shuarjes së zjarrit. Ai përcakton sasinë e pajisjeve dhe furnizimeve që droni mund të transportojë në vendin e zjarrit. Kapaciteti i ngarkesës ndryshon në varësi të madhësisë, dizajnit dhe peshës së dronit[21]. Për të kontrolluar kapacitetin e ngarkesës së dronit zjarrfikës, do të duhet të kryhen një sërë eksperimentesh që përfshijnë shtimin e ngarkesave të ndryshme në dronin dhe vëzhgimin se si funksionon. Më poshtë janë hapat e përfshirë në këtë proces:

1. Përcaktimi i peshës maksimale që mund të mbajë droni, duke përfshirë peshën e tij. Ky informacion zakonisht jepet nga prodhuesi i dronit.
2. Testimi, i cili fillon me një ngarkesë të lehtë që rritet gradualisht derisa droni mund të mos ngrejë më ose të lëvizë pa probleme.
3. Mbajtja në konsideratë e peshës së ngarkesës që droni mund të mbajë pa vështirësi. Ky do të jetë kapaciteti maksimali ngarkesës së dronit.
4. Përsëritja e testimit me lloje të ndryshme ngarkesash për të siguruar që droni mund të mbajë lloje të ndryshme të pajisjeve dhe furnizimeve.
5. Përgatitja e një raporti të shkurtër që përfshin specifikimet e dronit, peshën e ngarkesave të përdorura dhe rezultatet e eksperimentit dhe më pas bëhet kërkesa sipas nevojave dhe çmimeve të tregut.

---

[20] Guvenc, F. Koohifar, S. Singh, ML Sichitiu and D.Matolak, "Detection, Tracking and Stopping for Amateur Drones", Detection, Tracking and Stopping for Amateur Drones, Vol. 56, No. 4, pg. 75-81, 2018

[21] Maya, M., Castillo, E., Lomelí, A., GonzálezGalván, E., & Cárdenas, A. (2013). Workspace and payload-capacity of a new reconfigurable delta parallel robot. International Journal of Advanced Robotic Systems, 10(1), 56

6. Saktësia e dorëzimit.

Saktësia e një sistemi të shpërndarjes së dronëve zjarrfikës të krijuar për të hedhur ujë do të varet nga faktorë të ndryshëm si: dizajni i sistemit, aftësitë e dronit dhe kushtet në të cilat ai funksionon. Pas testimit, saktësia e sistemit mund të vlerësohet bazuar në shkallën e suksesit të dërgimit të ujit në zonën e synuar. Kjo mund të matet duke përdorur metrika të tilla si distanca midis zonës së synuar dhe zonës aktuale të rënies, vëllimi i ujit të dorëzuar në zonën e synuar dhe koha që duhet për të përfunduar shpërndarjen. Për të përmirësuar saktësinë, sistemi mund të rregullohet mirë në bazë të rezultateve të provës, duke rregulluar parametra të tillë si: shtegu i fluturimit të dronit, shpejtësia, lartësia dhe ngarkesa. Testimi dhe përsosja e vazhdueshme e sistemit mund të çojë në nivele më të larta saktësie me kalimin e kohës. Droni u zbulua se kishte një nivel të lartë të saktësisë së dorëzimit, i aftë për të hedhur ujë, rezistent ndaj zjarrit me saktësi në objektiva të madhësive dhe formave të ndryshme.[22] Kapaciteti i ngarkesës së dronit është paraqitur në figurën e mëposhtme.

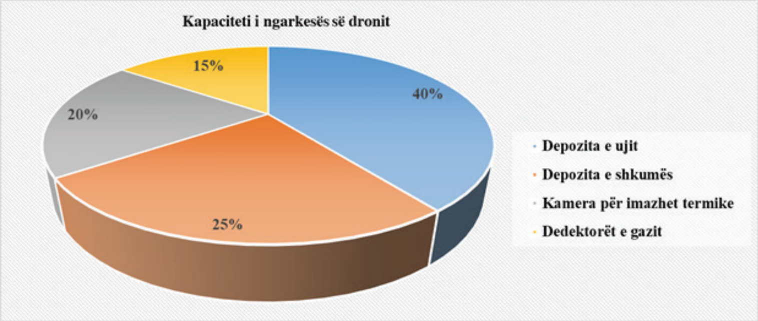


Figura nr. 2. Kapaciteti i ngarkesës së dronit.

7. Koha dhe diapazoni i fluturimit

Koha dhe diapazoni i fluturimit të një droni zjarrfikës mund të ndryshojnë në varësi të disa faktorëve të tillë si: kapaciteti i baterisë së dronit, pesha, kushtet e motit dhe kapaciteti i ngarkesës. Pas testimit, koha e fluturimit dhe diapazoni i një droni zjarrfikës mund të përcaktohet bazuar në specifikimet dhe aftësitë e tij specifike.

Për shembull, një dron me një kapacitet më të madh baterie zakonisht mund të fluturojë për një kohë më të gjatë se ai me një bateri më të vogël. Në mënyrë të ngjashme, diapazoni i dronit mund të ndikohet gjithashtu nga pesha e tij dhe kushtet e motit. Një dron më i rëndë mund të mos jetë në gjendje të fluturojë aq larg sa një dron më i lehtë dhe erërat e forta ose faktorë të tjerë mjedisorë mund të zvogëlojnë rrezen e dronit. Në përgjithësi, dronët e zjarrfikësve janë projektuar që të kenë një kohë fluturimi prej rreth 20-30 minuta dhe një distancë deri në disa kilometra. Sidoqoftë, koha dhe diapazoni i saktë i fluturimit do të varen nga modeli specifik i dronit dhe aftësitë e tij individuale. Droni u zbulua se kishte një kohë fluturimi deri në 25 minuta dhe një distancë deri në 2 kilometra[23].

---

[22] Deng, L., He, Y., & Liu, Q. (2019, October). Research on application of fire unmanned aerial vehicles in emergency rescue. In 2019 9th International Conference on Fire Science and Fire Protection Engineering (ICFSFPE) (pp. 1-5). IEEE.

8. Efektiviteti i shuarjes së zjarrit

Droni u zbulua se ishte shumë efektiv në shuarjen e zjarreve në lloje të ndryshme mjedisesh. Droni ishte në gjendje të shuante shpejt zjarret e madhësive dhe formave të ndryshme. Dronët e zjarrfikësve janë mjete ajrore pa pilot (UAV) të pajisura me aftësi për shuarjen e zjarrit si uji, shkuma ose kimikate të tjera.

Testimi i këtyre dronëve zakonisht përfshin vlerësimin e efektivitetit të shuarjes së zjarrit në mjedise të kontrolluara për të vlerësuar aftësinë e tyre për të shuar zjarret në mënyrë efikase dhe të sigurt[24]. Gjatë testimit, dronët e zjarrit zakonisht i nënshtrohen skenarë të ndryshëm zjarri, duke përfshirë zjarre të vogla, zjarre të mëdha dhe lloje të ndryshme zjarresh (të tilla si zjarre elektrike ose zjarre kimike). Dronët më pas kanë për detyrë të shuajnë zjarret duke përdorur pajisjet e tyre të zjarrfikësve në bord. Rezultatet e testimit zakonisht fokusohen në aftësinë e dronit për të shuar zjarrin në mënyrë efektive, si dhe në shpejtësinë dhe efikasitetin e tij për ta bërë këtë. Faktorë të tillë si sasia e ujit ose agjenti tjetër shuarës i përdorur, distanca midis dronit dhe zjarrit dhe saktësia e sistemit të synimit të dronit mund të merren parasysh të gjithë kur vlerësohet performanca e dronit.[25]

Testimi mund të vlerësojë gjithashtu aftësinë e dronit për të lundruar përmes tymit dhe pengesave të tjera për të arritur zjarrin, si dhe qëndrueshmërinë dhe besueshmërinë e tij të përgjithshme në kushte të ndryshme operimi. Në përgjithësi, rezultatet e testimit mund të ofrojnë njohuri të vlefshme për performancën e dronëve zjarrfikës dhe të ndihmojnë në përmirësimin e dizajnit dhe funksionalitetit të tyre. Duke vlerësuar efektivitetin e tyre në mjedise të kontrolluara, studiuesit dhe inxhinierët mund të identifikojnë fushat për përmirësim dhe të optimizojnë performancën e tyre për t'u përdorur në skenarët realë të shuarjes së zjarrit[26].

---

[23] Zadeh, N. R. N., Abdulwakil, A. H., Amar, M. J. R., Durante, B., & Santos, C. V. N. R. (2021). Firefighting UAV with shooting mechanism of fire extinguishing ball for smart city. Indones. J. Electr. Eng. Comput. Sci, 22, 1320-1326

[24] Borthakur, A., & Singh, P. (2016). Drones: new tools for natural risk mitigation and disaster response. Current Science, 110(6), 958.

[25] Alappatt, T. B., Ajith, S. S., Jose, J., Augustine, J., Sankar, V., & George, J. M. (2021). Design and Analysis of Fire Fighting Drone. In Advances in Electrical and Computer Technologies: Select Proceedings of ICAECT 2020 (pp. 1015-1033). Springer Singapore.

Përfundime

Ky shkrim paraqiti zhvillimet dhe testimet e një droni zjarrfikës të krijuar për të ndihmuar zjarrfikësit në situata të rrezikshme. Dizajni dhe zhvillimi i dronit u kryen duke përdorur teknika të avancuara të printimit 3D dhe simulime softuerësh, duke rezultuar në një dron të lehtë dhe të qëndrueshëm, i aftë për t'i bërë ballë kushteve ekstreme.

Aftësitë e dronit u testuan në një mjedis të kontrolluar, duke demonstruar efektivitetin e tij në shuarjen e zjarrit. Aplikimet e mundshme të dronit zjarrfikës në menaxhimin e fatkeqësive janë të rëndësishme. Droni mund të sigurojë monitorim dhe mbikëqyrje në kohë reale të zjarrit, duke ndihmuar zjarrfikësit në zhvillimin dhe marrjen e masave konkrete për eliminimin e vatrave ë zjarrit.

Bazuar në të dhënat eksperimentale të përdorimit të dronëve zjarrfikës, arrijmë në përfundimet e mëposhtme:

- Dronët e zjarrfikësve mund të përmirësojnë ndjeshëm efektivitetin dhe efikasitetin e operacioneve të shuarjes së zjarrit duke ofruar një zgjidhje inovative.
- Përdorimi i dronëve në operacionet e shuarjes së zjarrit mund të zvogëlojë rrezikun e lëndimit të zjarrfikësve duke eliminuar nevojën që ata të hyjnë në zona të rrezikshme.
- Dronët e pajisur me kamera të imazhit termik mund të identifikojnë shpejt pikat e nxehta dhe t'u ofrojnë zjarrfikësve të dhëna në kohë reale, duke i lejuar ata të marrin vendime të informuara dhe të rregullojnë strategjitë e tyre në përputhje me rrethanat.
- Përdorimi i dronëve në operacionet e shuarjes së zjarrit gjithashtu mund të zvogëlojë kohën e reagimit dukevlerësuar shpejt situatën dhe duke lejuar një dislokimmë të shpejtë të burimeve.
- Dronët e shuarjes së zjarrit tashmë kanë kaluar fazën eksperimentale dhe nuk kërkojnë testime dhe zhvillim të mëtejshëm për t'u bërë një mjet standard në operacionet e shuarjes së zjarrit.

---

[26] Barua, S., Tanjim, M. S. S., Oishi, A. N., Das, S. C., Basar, M. A., & Rafi, S. A. (2020, June). Design and implementation of fire extinguishing ball thrower quadcopter. In 2020 IEEE region 10 symposium (TENSYMP) (pp. 1404-1407). IEEE.

- Sfida të tilla si jetë gjatësia e baterisë, diapazoni dhe kapaciteti i ngarkesës duhet të adresohen për të përmirësuar efektivitetin dhe përdorimin e tyre.
- Përdorimi i dronëve mund t'i ndihmojë zjarrfikësit të kenë qasje dhe të vlerësojnë situatat e zjarrit shpejt dhe në mënyrë të sigurt, duke ofruar gjithashtu të dhëna dhe inteligjencë të vlefshme për të ndihmuar në informimin e strategjive të shuarjes së zjarrit. Analiza eksperimentale ka treguar se dronët e pajisur me kamera të imazhit termik mund të zbulojnë në mënyrë efektive pikat e nxehta dhe të ofrojnë reagime në kohë reale për zjarrfikësit. Për më tepër, përdorimi i dronëve mund të ndihmojë gjithashtu në përpjekjet e kërkimit dhe shpëtimit, pasi ata mund të skanojnë shpejt zona të mëdha dhe të identifikojnë çdo individ që ka nevojë për ndihmë.

Megjithatë, ka edhe disa kufizime dhe sfida që duhen adresuar, p.sh., dronët janë të ndjeshëm ndaj ndërhyrjeve nga sinjale të tjera me valë dhe mund të ndikohen nga kushtet e pafavorshme të motit si erërat e forta dhe shiu. Për më tepër, jetëgjatësia e baterisë së dronëve mund të kufizojë kohën dhe rrezen e tyre të funksionimit.

Si përfundim, analiza e dronëve zjarrfikës ka nxjerrë në pah potencialin e tyre për të përmirësuar operacionet e shuarjes së zjarrit dhe për të rritur sigurinë për zjarrfikësit. Ndërsa ka ende disa sfida për t'u kapërcyer, kërkimi dhe zhvillimi i vazhdueshëm në këtë fushë mund të çojë në përmirësimin e teknologjisë së dronëve të shuarjes së zjarrit.

Bibliografia

1. T. Markarian,"Unmanned aerial vehicles (drones) to prevent drowning, "Resuscitation, vol. 127, pp. 63– 67, 2018.
2. E. Lygouras, A. Gasteratos, K. Tarchanidis, Mitropoulos, A. ROLFER: "A fully autonomous aerial rescue support system,"Microprocess. Microsyst, vol. 61, pp. 32–42, 2018.
3. Y. LeCun, Y. Bengio, G. Hinton. "Deep Learning," Nature, vol. 521, pp. 436–444, 2018.
4. E. Petritoli, F. Leccese, L. Ciani, "Reliability and maintenance analysis of unmanned aerial vehicles," Sensors, vol. 18, pp. 56-71, 2018.
5. A. Adam, M. Elmaleeh, Mahmoud, D. "A smart neural network based algorithm for landing control of autonomous unmanned aerial vehicle," Int. J. Adv. Res. Sci. Eng, vol. 6, pp. 1175–1188, 2018.

6. K. Vijayakumar, S. Suchitra and P. Swathi Shri, “A secured cloud storage auditing with empirical outsourcing of key updates”, Int. J. Reasoning-based Intelligent Systems, Vol. 11, No. 2, 2019.
7. “Use of Fire-Extinguishing Balls for a Conceptual System of Drone-Assisted Wildfire Fighting”, Burchan Aydin, Emre Selvi, Jian Tao and Michael J. Starek, Published: 12 February 2019.
8. Yuan, C.; Zhang, Y.; Liu, Z. A survey on technologies for automatic forest fire monitoring, detection, and fighting using unmanned aerial vehicles and remote sensing techniques. Can. J. For. Res. 2015, 45, 783–792.
9. S. H. Alsamhi, O. Ma, S. M. Ansari, and S. K. Gupta, “Collaboration of Drone and Internet of Public Safety Things in Smart Cities: An Overview of QoS and Network Performance Optimization,” MDPI, vol. 3, 2019.
10. Death and destruction in the Philippines,” IFSEC PHILIPPINES, 2019.
11. J. L. Mayuga, “Tragedy of fires: Death and destruction in the Philippines,” The Broader Look, 21 march 2018.
12. Z. Guowei, Y. Su, Z. Guoqing, F. Pengyue and J. Boyan, “Smart firefighting construction in China: Status, problems, and reflections,” FAM fire and materials an international Journal, vol. 44, no. 4, no. 2020 John Wiley & Sons Ltd, pp. 516-529, 22 January 2020.
13. Cervantes et al., “A Conceptual Design of a Firefighter Drone,” in 2018 15th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE), Mexico City, Mexico, 2018.
14. J. Manley, “The Comeback of Fire Extinguishing Balls and their Benefits,” fire extinguisher pp. 101, 2019.
15. B. Aydin, E. Selvi, J. Tao and M. J. Starek, “Use of Fire-Extinguishing Balls for a Conceptual System of DroneAssisted Wildfire Fighting,” MDPI (drones), vol. 3, no. 17, 2019.
16. Vijayakumar, S. Suchitra and P. Swathi Shri, “A secured cloud storage auditing withempirical outsourcing of key updates”, Int. J. Reasoning-based Intelligent Systems,Vol. 11, No. 2, 2019.
17. Deng, L., He, Y., & Liu, Q. (2019, October). Research on application of fire uumanned aerial vehicles in emergency rescue. In 2019 9th International Conference on Fire Science and Fire Protection Engineering (ICFSFPE) (pp. 1-5). IEEE.
18. Kostoulas, P., Oteafy, S., &Chatzimisios, P. (2022, May). Fire-Fighting Drones: A Use Case for Tactile Internet. In ICC 2022-IEEE International

Conference on Communications (pp. 4613-4618). IEEE.

19. Jeyavel, J., Prasad, A. A., Shelke, K. M., Sargade, P. D., &Thoke, U. V. (2021, March). Survey on firefighting techniques using unmanned aerial vehicles. In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 239-241). IEEE.
20. Zadeh, N. R. N., Abdulwakil, A. H., Amar, M. J. R., Durante, B., & Santos, C. V. N. R. (2021). Fire- fighting UAV with shooting mechanism of fire extinguishing ball for smart city. Indones. J. Electr. Eng. Comput. Sci, 22, 1320-1326.
21. Yao, Q., Qiu, J., Fan, Y., & Yan, W. (2021, May). Quad-rotor fire-fighting drone based on multifunctional integration. In 2021 International Conference on Artificial Intelligence and Electromechanical Automation (AIEA) (pp. 70-73). IEEE.
22. Alappatt, T. B., Ajith, S. S., Jose, J., Augustine, J., Sankar, V., & George, J. M. (2021). Design and Analysis of Fire Fighting Drone. In Advances in Electrical and Computer Technologies: Select Proceedings of ICAECT 2020 (pp. 1015-1033). Springer Singapore.
23. Yuan, Y. (2021, April). Technical Research on Fire- Fighting Robotics. In 2021 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC) (pp. 140-143). IEEE.
24. Barua, S., Tanjim, M. S. S., Oishi, A. N., Das, S. C., Basar, M. A., & Rafi, S. A. (2020, June). Design and implementation of fire extinguishing ball thrower quadcopter. In 2020 IEEE region 10 symposium (TENSYMP) (pp. 1404-1407). IEEE.
25. Fuller, S. B. (2019). Four wings: An insect-sized aerial robot with steering ability and payload capacity for autonomy. IEEE Robotics and Automation Letters, 4(2), 570-577.
26. Parkavi G, Daphine Desona Clemency C A, Rehash Rushmi Pavitra A, P. Uma Maheswari, I. Daniel Lawrence, 2023. Internet of Things (IoT) Enabled Cloud Computing Drone for Smart Agriculture: Superior Growth and Life. Journal of Population Therapeutics and Clinical Pharmacology, 30(12), pp.256-262.
27. Rehash Rushmi Pavitra A, Parkavi G, Uma Maheswari P, Karthikeyan K, Daniel Lawrence I, 2022. An Illustrative Review on Machine Learning Techniques along with Software Tools and its Evaluation. NEUROQUANTOLOGY, 20(16), pp.233-236.

28. Daniel Lawrence I, Vijayakumar R, Agnishwar J, (2023). Dynamic Application of Unmanned Aerial Vehicles for Analyzing the Growth of Crops and Weeds for Precision Agriculture. Artificial Intelligence Tools and Technologies for Smart Farming and Agriculture Practices. Pages: 115-132. DOI: 10.4018/978-1-6684-8516-3.ch007.

Siguria dhe qëndrueshmëria kibernetike e aviacionit. Vlerësimi i rrezikut në menaxhimin e trafikut ajror

Laureta BETA
Specialiste në Drejtorinë e Trajnimit dhe Licencimit, ALBCONTROL

Trajtesë e shkurtuar.

Në shumë industri, përdorimi dhe integrimi i teknologjisë dhe digjitalizimi nga njëra anë kanë sjellë avantazhe të panumërta, por nga ana kanë sjellë një rrezik më të madh që diçka të mos shkojë mirë. Kërcënimet e sigurisë ndaj operacioneve të aviacionit civil janë bërë sot më të sofistikuara dhe sfiduese. Një fenomen i cili po shfaqet gjithnjë e më shumë vitet e fundit, ndoshta edhe më i avancuar e më i ndërlikuar për t'u menaxhuar, është sulmi kibernetik.

Sot, komuniteti global i aviacionit civil po mbështetet në sistemet kompjuterike dhe të Teknologjisë së Informacionit (IT) për operacionet e tyre të përditshme qoftë në "vijën e parë" apo dhe për operacionet në "prapavijë". Kjo mbështetje pritet të rritet ndërsa aeroportet e reja dhe moderne zhvillohen, avionët e rinj futen në shërbim dhe palët e interesuara kërkojnë të plotësojnë kërkesën në rritje të pasagjerëve më të aftë të IT për lehtësimin e proceseve të pasagjerëve, duke përdorur sisteme digjitale dhe të bazuara në IT[1]*. Kështu që nëse nuk zbatohen masat e duhura të sigurisë në fuqi, hakerat mund të aksesojnë lehtësisht informacionin tuaj. Kjo nxjerr në pah rëndësinë e enkriptimit siç duhet të të dhënave dhe kjo është veçanërisht e vërtetë në industrinë e aviacionit, nga*

---

[1] Lim B. Siguria e aviacionit - kërcënimet e reja nga siguria kibernetike në aviacion - sfidat dhe masat zbutëse. J Aviat Manag

oraret dhe itineraret deri tek informacioni i transportit tokësor dhe informacionet personale. Ashtu si çdo industri dhe ajo e aviacionit civil përballet me sfida për sigurinë kibernetike po aq të mëdha sa në të tjerat.

Aktualisht aviacioni civil është mënyra më e sigurt e transportit në botë dhe ndoshta edhe sistemi më i ndërlidhur i teknologjisë së informacionit dhe komunikimit. Sulmet kibernetike po rriten në sasi dhe qëndrueshmëri, kështu që pasojat e një sulmi të suksesshëm keqdashës kibernetik ndaj operacioneve të aviacionit civil mund të jenë të rënda. Teknologjitë e reja, zgjerimi i lidhjeve dhe integrimi i tyre në industrinë e aviacionit, veçanërisht në fushën e Menaxhimit të Trafikut Ajror (MTA) (Air Traffic Management-ATM), rrisin rrezikun për këto asete kritike. Përdorimi i IT në aviacionin civil është rritur çdo vit, ndërsa në vitet e fundit është rritur eksponencialisht.

Digjitalizimi, mjetet teknologjike dhe sistemet e lidhura shpesh me internetin rrisin inteligjencën dhe ndërveprueshmërinë nga njëra anë, ndërsa nga ana tjetër mund të përbëjnë rreziqe serioze për sigurinë kibernetike të aviacionit. Prandaj, është e nevojshme të mbahet një nivel i lartë i vëmendjes dhe ndërgjegjësimit për zhvillimet e mundshme të ardhshme të kërcënimit kibernetik[2]*.*

Qëllimi final është të reduktohet cënueshmëria ndaj rreziqeve të lidhura me kibernetikën, të forcohet qëndrueshmëria e sistemeve të transportit ajror ndaj këtyr kërcënimeve, e cila shihet si aftësia e një sistemi organizativ dhe teknik për të mbrojtur veten nga dështimet/humbjet dhe zbutur ndikimet duke u përshtatur ndaj ndryshimit të kushteve dhe rikuperimit nga degradimi pas incidentit[3]*. Sigurisht që sfidat, shqetësimet lidhur me kërcënimet kibernetike të sigurisë në sektorin e aviacionit janë të lidhura ngushtësisht me analizën e masave të sigurisë kibernetike dhe praktikat në funksion të përmirësimit të elasticitetit kibernetik të aeroporteve me qëllim adresimin e dobësive ekzistuese dhe të varësive*[4]*.*

Fjalë kyçe: siguria kibernetike e aviacionit, rezistenca kibernetike e aviacionit, kërcënimet kibernetike të MTA, shërbimet e navigimit ajror dhe siguria kibernetike etj.

---

[2] De Zan T, d'Amore F, Di Camillo F (2015) Mbrojtja e sistemeve të trafikut ajror civil nga kërcënimet kibernetike.

[3] Kreuzer M, Kiesling T (2017) Rekomandime për forcimin e qëndrueshmërinë kibernetike të sistemit të trafikut ajror, ARIEL,Qëndrueshmëria e trafikut ajror.

[4] Lykou G, Anagnostopoulou A, Gritzalis D (2018) Zbatimi i masave të sigurisë kibernetike në aeroporte për të përmirësuar qëndrueshmërinë kibernetike, WIIoTS në Samitin e Dytë Global të Internet of Thinks (IoT)

Hyrje

Siguria kibernetike është akti i mbrojtjes së çdo lloj teknologjie nga një sulm digjital dhe mund të përfshijë: kompjuterët, serverët, pajisjet mobile, sistemet elektronike, rrjetet dhe të dhënat. Ndërsa bota bëhet gjithnjë e më e digjitalizuar, shanset për të "vuajtur" nga një lloj sulmi digjital rriten. Shpeshherë, kohët e fundit, përmendet sulmi më i ri ransomware ose shkelja e të dhënave. Sa herë që një kompjuter ose server sulmohet nga hakerat, konsiderohet si një sulm kibernetik. Dy nga llojet më të njohura të sulmeve kibernetike njihen si ransomware dhe rrjedhja e të dhënave. Sulmet ransomware ndodhin kur hakerat kërcënojnë të publikojnë të dhëna të ndjeshme ose të bllokojnë përgjithmonë aksesin në të, derisa të paguhet një shpërblim i caktuar. Sulmet ransomware mund të prekin jo vetëm kompanitë, por edhe njerëzit. Një tjetër lloj i zakonshëm i sulmit kibernetik është shkelje/ rrjedhje e të dhënave. Kjo ndodh kur informacioni konfidencial/ndjeshëm ekspozohet apo ndahet pa leje. Një shembull popullor është ekspozimi në *facebook* (në vitin 2019) i informacioneve personale, emrave dhe numrave të telefonit. Ashtu si *facebook*-u dhe industria e aviacionit, si çdo industri tjetër në botë, është në rrezik për sulme kibernetike pasi kjo industri digjitalizohet vijimisht me avantazhet dhe dizavantazhet e saj. Gjithësesi, rreziku i sigurisë kibernetike është një sfidë relativisht e re për aviacionin.

Përdorimi në rritje i teknologjisë në aviacionin civil i lejon ata të trajtojnë disa nga sfidat e tanishme që po hasen. Ekziston mundësia për një planifikim më të efektshëm fluturimi kur gjithçka është digjitale por, një nga sfidat më të mëdha në industri është karburanti, për të cilin po bëhen përpjekje që të reduktohen emetimet dhe konsumi. Epoka digjitale mund të ndihmojë edhe në trajnimin e punës dhe të sigurisë së punonjësve. Fatkeqësisht, të gjitha avantazhet shoqërohen me një kosto. Avionët e aktivizuar elektronikë po kthehen sot në qendra të dhënash fluturuese. Me avionët që po bëhen plotësisht digjitalë, gjithçka po bëhet më e ndërlidhur. Kjo do të thotë se për hakerët potencialë ka më shumë "dyer që hapen". Përdorimi në rritje i softuerit komercial i lehtëson hakerët të kenë akses sepse ata nuk kanë nevojë për njohuri specifike të aviacionit për të sulmuar sisteme që janë shumë të ngjashme me ato që përdoren në industritë e tjera. Për shkak se ka kaq shumë sisteme të ndryshme që kanë nevojë për mbrojtje, mund të jetë e vështirë të mbulohen të gjitha bazat. Rritja e sasisë së teknologjisë dhe digjitalizimit në aeroplanë, po shkon në përjestim të drejtë dhe me atë në aeroporte. Për arsye se ka kaq shumë sisteme dhe teknologjia moderne po avancon, personeli nuk është i trajnuar mjaftueshëm për të përballuar këto sfida të reja.

Me kalimin e kohës dhe vendosjen e masave më të mira të sigurisë, dhe punonjësit e aeroporteve, dhe ata të linjave ajrore do të fitojnë trajnimin dhe përvojën e nevojshme, gjë e cila do të ulë mundësinë për sulme kibernetike. Por si çdo industri tjetër, pavarësisht se çfarë rregullash sigurie vendosen dhe zbatohen, gjithmonë do të ketë shanse për sulm. Kjo kërkon që personeli duhet të sigurohet që sistemet funksionojnë dhe në avion zbatohet teknologjia e re. Kjo vlen më tepër për teknikët e mirëmbajtjes së aviacionit (ata që janë në prapaskenë), të cilët duhet të sigurojnë që elektronika, ndër të tjera në avionë, të jetë në rregull.

Ekosistemi i aviacionit është kompleks, dhe i ndërtuar me shumë blloqe të ndryshme; p.sh., komponentët kryesorë të infrastrukturës së këtij ekosistemi përfshijnë Menaxhimin e Trafikut Ajror (ATM), i cili përfshin sisteme të ndryshme komunikimi, lundrimi dhe vëzhgimi (Communication, Navigation, and Surveillance-CNS). Sistemet e komunikimit në përgjithësi përfshijnë pajisje që lehtësojnë shkëmbimin e informacionit (p.sh., komandat, zëri dhe informacione të tjera të të dhënave) midis pajisjeve, sistemeve dhe përdoruesve (p.sh., Kontrolli i Trafikut Ajror (ATC) dhe piloti), (p.sh. sistemet dhe radarët në bord), dhe infrastruktura mbështetëse të cilat lehtësojnë mbikëqyrjen. Shembuj të sulmeve në komunikim janë ato që synojnë sinjalet e komunikimit (p.sh., bllokimi i sinjalit apo të dhënat e rreme). Sulmet e lidhura me lundrimin përfshijnë mashtrimin ose bllokimin e GPS, bllokimin dhe përgjimin e sinjalit, sulmet e modifikimit të lundrimit dhe ato të lidhura me mbikëqyrjen ku përfshihen ata që kërkojnë të kryejnë mbikëqyrje të paautorizuar të avionëve dhe lëvizjeve të tyre, bllokimin, modifikimin si dhe fshirjen e sinjalit.

Aktualisht aviacioni është një bazë kyçe për tregtinë ndërkombëtare, turizmin dhe investimet thelbësore për zhvillimin e ekonomisë globale. Industria e transportit ajror mbështet rreth 2.7 trilion dollarë ose 3.5% të produktit të brendshëm botëror bruto (PBB) me rreth 10 milionë vende pune direkt në industrinë e transportit ajror[5]. Nga disa parashikime, deri në vitin 2034, si trafiku ajror i pasagjerëve ashtu edhe ai i mallrave pritet të dyfishohen, krahasuar me vitin 2016. Trafiku i pasagjerëve pritet të rritet me rreth 4.5% në vit, ndërsa ai i mallrat me rreth 4.2% në vit.[6]

1. Kuptimi i ndërveprimit të MTA

Për të menaxhuar në mënyrë të sigurt hapësirën ajrore nga Kontrolli i Trafikut Ajror, çdo kontrollues i trafikut ajror duhet të kuptojë statusin e çdo avioni nën kontrollin e tij. Tradicionalisht, Radarët e Mbikëqyrjes Parësore dhe Dytësore në planimetri të ndryshme kanë mbështetur mbikëqyrjen dhe menaxhimin e trafikut ajror për dekada të tëra. Të dy sistemet u projektuan në një kohë kur transmetimi i radios kërkonte një investim dhe ekspertizë të madhe financiare. Prandaj, asnjë mendim për sigurinë nuk iu kushtua këtyre sistemeve të trashëguara, pasi supozohej se ato do të mbeteshin jashtë mundësive. Rritja e Radio Defined Software (SDR) e anuloi këtë supozim dhe shënoi kalimin nga sulmuesit e mundshëm që kishin burime të mira në ata me burime dhe aftësi shumë më të pakta[7].

---

[5] Grupi i Nivelit të Lartë të Industrisë (Industry High-Level Group-IHLG) Raporti i përfitimeve të aviacionit 2017.

[6] Grupi i Nivelit të Lartë të Industrisë (2017) Raporti i përfitimeve të aviacionit 2017.

Lëvizja e vazhdueshme nga sistemet tradicionale të kontrollit të trafikut ajror, si radari dhe zëri, drejt sistemeve të përmirësuara të mbikëqyrjes dhe komunikimit duke përdorur rrjete moderne të të dhënave, ka shkaktuar një ndryshim thelbësor në sigurinë e mjedisit të aviacionit. Zbatuar përmes programeve të kërkimit të aviacionit si Single European Sky MTA Research dhe programet amerikane NextGen (the US American NextGen programs), disa protokolle të reja të kontrollit të trafikut ajror dhe komunikimit janë duke u zhvilluar aktualisht, dhe pse këto protokolle kanë qenë në punë për dekada[8]. Këtu përshkruhen shkurtimisht sistemet bazë të MTA-ve që shërbejnë për mbikëqyrjen dhe ndërveprueshmërinë, të përdorura për kontrollin e trafikut ajror si: Radari i Mbikëqyrjes Primar dhe Sekondar, Mbikëqyrja-Transmetimi i Varur Automatik, Sistemi i Përplasjeve dhe Shmangies së Trafikut dhe Multilateralizimi në Zonë të Gjerë. Të gjitha këto sisteme ndërveprojnë me njëri-tjetrin siç paraqitet grafikisht në fig. 1.

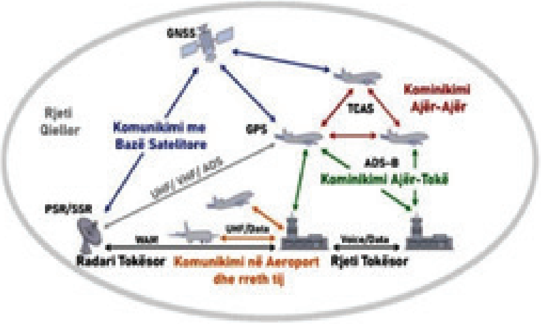


Figura nr. 1
Ndërveprueshmëritë e MTA

Më poshtë do të shohim se si përparimet e fundit në teknologjitë me valë kanë ndryshuar peizazhin e kërcënimit në kontekstin e aviacionit. Radari Primar i Mbikëqyrjes (Primary Surveillance Radar-PSR) përshkruan sistemet e lokalizimit të radarëve jobashkëpunues. Në aviacionin civil, këto zakonisht përdorin një antenë rrotulluese që rrezaton një rreze elektromagnetike të moduluar nga pozicioni i pulsit dhe me drejtim të lartë në një brez të ulët GHz.

---

[7] Strohmeier M et al (2014) Realitetet dhe sfidat e menaxhimit të trafikut ajror të ardhshëm: rasti i ADS-B. IEEE Communations Magazine 52(5):111–118.

[8] Strohmeier M et al (2016) Vlerësimi i ndikimit të sigurisë së aviacionit në fuqinë kibernetike. Konferenca e 8 ndërkombëtare për fuqinë kibernetike të konfliktit kibernetik.

Objektivat e mundshëm në hapësirën ajrore pasqyrojnë pulset dhe matja e kohës së mbajtjes dhe vajtje-ardhjet e këtyre reflektimeve sigurojnë pozicionin e objektivit. Ndërsa PSR nuk është i pasur me të dhëna, është relativisht e vështirë të sulmohet pasi mbështetet në vetitë fizike[9].

Radari Sekondar i Mbikëqyrjes (Secondary Surveillance Radar - SSR) është një teknologji bashkëpunuese me versione moderne të komunikimit, duke përfshirë të ashtuquajturat mënyra të transponderit. SSR ofron më shumë informacion të synuar në ekranet e radarëve ATC në krahasim me PSR. Stacionet tokësore marrin në pyetje transponderët e avionëve duke përdorur mesazhe digjitale në frekuencën 1030 MHz, të cilat përgjigjen me informacionin e duhur në kanalin 1090 MHz. Pajisjet e mallrave mund të marrin dhe transmetojnë në këto frekuenca, duke i bërë ato të aksesueshme për sulm[10]. Modaliteti S është veçanërisht i rëndësishëm për sistemin aktual SSR. Ai mbështet sisteme me rëndësi në rritje në mbikëqyrjen moderne të aviacionit, në lidhje me teknikat e shumëfishta. Duke qenë të dizajnuara qëllimisht me mungesë konfidencialiteti, të gjitha sistemet SSR janë subjekt i sulmeve të përgjimit nga vëzhguesit pasivë[11]. Transmetimi Automatik i Mbikëqyrjes së Varur (Automatic Dependent Surveillance-Broadcast-ADS-B) është një protokoll në të cilin avionët transmetojnë vazhdimisht identifikimin (ID) e tyre, pozicionin dhe shpejtësinë e tyre, si dhe informacione të mëtejshme si kodet e qëllimit ose urgjencës.

Këto transmetime nuk kërkojnë marrje në pyetje, por dërgojnë në mënyrë të pavarur pozicionin dhe shpejtësinë e avionit dy herë në sekondë dhe identifikimin unik në çdo 5 sek; ADS-B është aktualisht në fazën e lëshimit dhe është i mandatuar për përdorim nga të gjithë avionët që nga viti 2020 në të gjithë hapësirën ajrore evropiane dhe amerikane[12]. Sistemi i Shmangies së Trafikut dhe Përplasjes (Traffic Collision and Avoidance System-TCAS) lejon avionët të marrin në pyetje avionët e afërt, për të zgjidhur konfliktet në hapësirën ajrore. Psh, nëse një avion tjetër hyn brenda një diapazoni të paracaktuar, TCAS fillimisht do të prodhojë një Këshillim për Trafikun që njofton pilotin për trafikun aty pranë. Nëse ndërhyrësi hyn në hapësirën e menjëhershme ajrore të avionit, do të krijohet një alarm që udhëzon njërin prej avionëve të ndryshojë kursin. Që nga fillimi i dhjetorit 2015, TCAS është i mandatuar për t'u përfshirë në avionët civilë që transportojnë më shumë se 19 pasagjerë ose me një peshë minimale ngritjeje prej 5700 kg[13]. Multilatimi i sipërfaqes së gjerë (Wide Area Multilateration-WAM) është veçanërisht i dobishëm për MTA pasi lejon vlerësimin e vendndodhjes së një avioni duke përdorur mesazhe 1090 MHz në zona të mëdha. WAM, i kombinuar me ADS-B, do të formojë një pjesë kyçe të teknologjive të mbikëqyrjes së gjeneratës së ardhshme[14] dhe mund të ndihmojë në zbulimin e raporteve të pazakonta ADS-B. Për shkak të numrit të sensorëve dhe pajisjeve të përpunimit të të dhënave që kërkohen për të mbuluar zona të mëdha, kostoja e instalimit është shumë e lartë, kjo e bën WAM mjaft të vështirë për t'u sulmuar. Për të grumbulluar informacionin, të gjitha sistemet e mësipërme të mbikëqyrjes të MTA me karakteristikat, varësitë dhe dobësitë e përmendura janë paraqitur në tabelën nr. 1.

---

[9] Strohmeier M et al (2016) Mbi perceptimin dhe realitetin në sigurinë e komunikimeve të trafikut ajror wireless.

[10] Costin A, Francillon A (2012) Fantazma është në ajër (trafiku): mbi pasigurinë e protokollit ADS-B dhe sulmet praktike në pajisjet ADS-B.

[11] Strohmeier M et al (2016) Vlerësimi i ndikimit të sigurisë së aviacionit në fuqinë kibernetike. Konferenca e 8 ndërkombëtare për fuqinë kibernetike të konfliktit kibernetik.

[12] Strohmeier M et al (2016) Vlerësimi i ndikimit të sigurisë së aviacionit në fuqinë kibernetike. Konferenca e 8 ndërkombëtare për fuqinë kibernetike të konfliktit kibernetik.

Sistemi	**Varësia Tokë/ ajër**	**Statusi i vendosjes**	**Teknologjia**	**Varësia**	**Dobësia**
Radari Primar i Mbikëqyrjes (PSR)	Tokë	Në përdorim	Mat mbajtësen dhe distancën e objektivave duke përdorur reflektime të shkëputura të sinjaleve radiofonike	Objektivi i avionit i pavarur	Jo e lidhur me IT
Radari Sekondar i Mbikëqyrjes (SSR)	Tokë	Në përdorim	Kërko informacion shtesë nga aeroplani si identiteti, lartësia, shpejtësia	Objektivat e pajisura me transponder	Përgjimi
Përplasja e Trafikut dhe Sistemi i Shmangies (TCAS)	Ajër	Në përdorim/ e detyrueshme nga 2015	Marrja në pyetje e identitetit të synuar	Objektivat e pajisura me transponder	Përgjimi, bllokimi, mashtrimi

---

[13] Rregullorja e Komisionit Evropian (2011) që përcakton kërkesat e përbashkëta të përdorimit të hapësirës ajrore dhe procedurat e funksionimit për shmangien e përplasjeve ajrore, nr. 1332 BE.

[14] Organizata Ndërkombëtare e Aviacionit Civil (ICAO) (2013) Aftësia fillestare për mbikëqyrjen tokësore. Në planin global të navigimit ajror 2013–2028.

Transmetimi automatik i varur i mbikëqyrjes (ADS-B)	Ajër	Mandatuar nga 2020	Objektivat e transmetimit të informacionit në lidhje me identitetin, lartësinë, shpejtësinë.	Objektivat e pajisura me transponder	Përgjimi, bllokimi, mashtrimi
Zona e gjerë multilaterale (WAM)	Tokë	Në vendosje	Kombino ADS me PSD SSR Të dhëna për qëndrueshmëri	Përpunimi qendror i IT bazuar në informacion	Përpunimi i të dhënave dhe lidhja me IT

Tabela nr. 1
Karakteristikat, varësitë dhe dobësitë e sistemit të menaxhimit të trafikut ajror

2. Agjentë të kërcënimeve kibernetike të aviacionit

Megjithëse transporti ajror ka një histori të gjatë të menaxhimit të rrezikut me fokus të veçantë në sigurinë fizike, fusha e rreziqeve kibernetike ka prezantuar së fundmi një peizazh të ri kërcënimesh. Në vitin 2016, në Asamblenë e 39-të, ICAO, ka shpallur punimet përgatitore për sigurinë dhe qëndrueshmërinë kibernetike. Në këtë drejtim, kapitulli i 18-të i Manualit të Sigurisë së Aviacionit i cili trajton kërcënimet kibernetike është përditësuar në shtator 2017. Për më tepër, Manuali i Sigurisë së Aviacionit (Dokumenti 8973) është përmirësuar për të ofruar udhëzime, duke përfshirë masat minimale, për të mbrojtur sistemet kritike të informacionit ndaj aksesit të paautorizuar dhe përdorimit.[15]

Përveç kësaj, studimet e fundit kërkimore kanë zbuluar se kërcënimi kibernetik ka shumë të ngjarë të jetë një nga çështjet kryesore të sigurisë në aviacion, pasi sipas programeve SESAR dhe NextGen, sistemi i përgjithshëm i transportit ajror do të migrojë masivisht në një infrastrukturë të bazuar në IP dhe do të funksionojë në përputhje me rrjetin qendror (koncepti i operacioneve, me ndarjen e informacionit në kohë reale[16]). Si një burim kritik, informacioni duhet të trajtohet si çdo aset tjetër kritik që është thelbësor për efikasitetin dhe ofrimin e suksesshëm të sistemeve MTA.

Në fushën e sigurisë kibernetike të aviacionit, puna kërkimore ka treguar se kompleksiteti dhe siguria e informacionit kritik dhe menaxhimit të tij kërkojnë nivelin më të lartë të sigurisë organizative. Organizata Civile e Shërbimeve të

---

[15] ICAO (2013) Aftësia fillestare për mbikëqyrjen tokësore. Në planin global të navigimit ajror 2013-2028.

[16] Kreuzer M, Kiesling T (2017) Rekomandime për forcimin e qëndrueshmërinë kibernetike të sistemit të trafikut ajror, ARIEL,Qëndrueshmëria e trafikut ajror.

Navigimit Ajror (CANSO) ka nxjerrë në 2014 një udhëzues për Sigurinë Kibernetike[17] duke shpjeguar se si ofruesit e shërbimeve të navigimit ajror duhet të marrin parasysh rreziqet e sigurisë kibernetike në menaxhimin e trafikut ajror, duke përfshirë kërcënimet kibernetike, dobësitë, motivet e aktorëve të kërcënimit, si dhe konsideratat në lidhje me menaxhimin e këtyre rreziqeve dhe zbatimin e një programi të sigurisë kibernetike. Sathish et al[18] propozoi një kornizë vlerësimi të cenueshmërisë për kërcënimet me valë në Sistemet Kibernetike të Aviacionit (ACPS) duke vlerësuar mjetet dhe i përdori ato për të vlerësuar kërcënimet që lidhen me ACPS.

Sampigethaya et al.[19] paraqiti një studim gjithëpërfshirës të sigurisë së aeroplanit të aktivizuar elektronik me aplikacione të tilla si shpërndarja elektronike e softuerit dhe të dhënave të ngarkueshme, si dhe drejtimet e ardhshme si kontrolli i rrjetit pa tel dhe rrjetet ajrore *ad hoc*.

Nëpërmjet qasjes së tij, Bernard Lim[20] shikon disa nga sfidat dhe mënyrat e mundshme për të adresuar shqetësimin e kërcënimeve të sigurisë kibernetike me të cilat përballet komuniteti global i aviacionit civil. Gjatë studimit të tyre, Stander dhe Ophoff[21] zbuluan se janë ndërmarrë hapa nga prodhuesit e avionëve dhe organet kontrolluese për të parandaluar shfaqjen e incidenteve për të komprometuar sistemet e informacionit të një avioni. D. Jeyakodi[22] justifikon në punimin e saj se si industria globale e aviacionit do të mbetet një objektiv për kundërshtarët që kërkojnë të bëjnë një deklaratë ose të shkaktojnë humbje të konsiderueshme në jetë dhe në gjendje financiare. Çelësi për të garantuar sigurinë do të ishte mbajtja në hap me zhvillimet, duke qenë kështu në një pozicion për t'u përballur me kërcënimet në vend që të evokohen veprime të përgjegjshme pas saj dukurie.

Strohmeier M.[23] ka paraqitur një model realist të kërcënimit bazuar në aftësitë e përditësuara të llojeve të ndryshme të agjentëve të kërcënimit dhe ndikimin e tyre në sistemin e digjitalizuar të komunikimit të aviacionit, ku agjentët kërcënues klasifikohen në bazë të motivimit dhe aftësive të tyre. Së fundi këtyre modeleve i është shtuar një kërcënim i ri: “Insajderi”. Besohet fuqishëm se ky aktor mbetet një agjent i konsiderueshëm kërcënimi dhe nuk duhet neglizhuar. Është vlerësuar gjithashtu ekspozimi ndaj rrezikut, duke marrë parasysh kontrollet e sigurisë të zbatuara dhe zgjidhjet si dhe kundërmasat e disponueshme të sigurisë, të propozuara.

---

[17] CANSO (2014) Siguria kibernetike dhe vlerësimi i rrezikut Organizata e Shërbimeve të Navigacionit Ajror Civil.

[18] Kumar S, Xu B (2017) Vlerësimi i cenueshmërisë për sigurinë në sistemet kibernetike-fizike të aviacionit. Konferenca e 4-të ndërkombëtare e IEEE mbi sigurinë kibernetike dhe mjedisin virtual.

[19] Sampigethaya K, Poovendran R, Bushnell L (2008) Funksionimi, kontrolli dhe mirëmbajtja e sigurt e aeroplanëve të ardhshëm, Laboratori i Sigurisë së Rrjetit (Network Security Lab-NSL), Departamenti EE, Universiteti i Washingtonit, Seattle.

[20] Lim B (2014) Siguria e aviacionit-kërcënimet e shfaqura nga siguria kibernetike në aviacion-sfidat dhe masat zbutëse, J Aviat Manag

[21] Stander A, Ophoff J (2016) Siguria kibernetike në aviacionin civil

[22] JeyakodiD (2015) Siguria kibernetike në aviacionin civil

[23] Strohmeier M et al (2016) Vlerësimi i ndikimit të sigurisë së aviacionit në fuqinë kibernetike. Konferenca e 8 ndërkombëtare për fuqinë kibernetike të konfliktit kibernetik.

- ***Vëzhguesit pasivë,*** shfrytëzojnë natyrën e hapur të protokolleve të komunikimit të trafikut ajror. Ata përdorin faqet e internetit si publike ashtu dhe private dhe aplikacionet celulare, të cilat shfaqin trafikun ajror dhe komunikimet e tij në kohë reale, për të mbledhur informacione rreth lëvizjeve private ose sekrete të trafikut ajror. Ata mund të përdorin marrës të lirë SDR për të mbledhur pamjen e tyre të pa shtrembëruar të të gjithë trafikut ajror në afërsi, në kohë reale ose të ruajtur për analiza të mëvonshme. Informacioni i grumbulluar mund të përdoret në shumë mënyra, duke filluar nga shqetësimet e privatësisë deri te zbulimi i operacioneve ushtarake. Ekspozimi ndaj rrezikut të sistemeve MTA në agjentë të tillë kërcënimi është mjaft i ulët, për shkak të mungesës së aftësive sulmuese në industrinë e aviacionit.

- ***Aktivistët dhe hobiistët,*** janë kërcënimi më i ulët aktiv i cili bazohet në aftësitë e tyre në lidhje me harduerin dhe njohuritë. Qëllimi i tyre është të shfrytëzojnë hapësirat e sigurisë me sulme ekzistuese, të lehta për t’u përdorur dhe me sofistikim tipik të ulët ku ata janë në gjendje të monitorojnë dhe ndërhyjnë në kanalet e komunikimit të aviacionit. Motivimi i tyre rregullisht nuk është racional, përkundrazi, çdo ndikim i identifikueshëm kërkohet për publicitet, emocion dhe njohje[24]. Rreziku i sistemeve MTA nga agjentë të tillë konsiderohet i ulët, pasi ato mund të zbulohen dhe zbuten me përdorimin e sistemeve të mbikëqyrjes rezervë.

- ***Personat e brendshëm,*** mund të jenë një kërcënim serioz dhe shpesh janë punonjës të pakënaqur, ish-punonjës, kontraktorë, apo edhe bashkëpunëtorë biznesi. Këta përdorues kanë informacion të brendshëm të praktikave të sigurisë, të dhënave dhe sistemeve kompjuterike të organizatës. Fakti që një person i brendshëm ka akses në aplikacionet kryesore dhe sistemet e tjera kritike e bën atë potencialisht edhe më të rrezikshëm se kriminelët kibernetikë të palëve të treta që përpiqen të depërtojnë përmes malware dhe mekanizmave të tjerë. Prandaj, ekspozimi ndaj rrezikut të sistemeve të MTA-ve është mesatar, pasi është vërtet e vështirë të zbulohen menjëherë qëllimet ose veprimet keqdashëse të personit të brendshëm.

---

[24] Theocharidou M (2016) D1.3 - leksiku përfundimtar i përkufizimeve në lidhje me elasticitetin e infrastrukturës kritike, Kërkimi horizont 2020 i BE.

- ***Sulmuesit e krimit kibernetik,*** zakonisht kërkojnë të sulmojnë sistemet për përfitime monetare, duke pasur njohuri të mjaftueshme, duke përdorur radio të përcaktuara me softuer, madje edhe mjete të vogla ajrore pa pilot (UAV), duke qenë në gjendje të injektojnë mesazhe të reja ose të modifikojnë ato ekzistuese në mënyra të tilla që ata nuk janë të shënuara nga sistemet aktuale të zbulimit. Ata përpiqen të shkaktojnë dëme maksimale dhe të ushtrojnë kërcënime të besueshme, si parakusht për shantazh ose për të përfituar nga njohuritë e brendshme. Për rrjedhojë, ata kërkojnë të shfrytëzojnë çdo mënyrë të mundshme dhe efektive për të sulmuar kontrollin e trafikut ajror dhe sistemet e avionëve. Ekspozimi ndaj rrezikut të sistemeve MTA është mesatar dhe duhet të merret seriozisht në konsideratë në vlerësimet e rrezikut të kryera rregullisht.

- ***Kiber-terroristët,*** (terroristët kibernetikë) kërkojnë të kërcënojnë sigurinë kombëtare, të shkaktojnë viktima masive, të dobësojnë ekonominë dhe të dëmtojnë moralin dhe besimin publik në sistemet e aviacionit[25]. Duke shfrytëzuar dobësitë në komunikimet e aviacionit, grupet terroriste, të cilat tradicionalisht rrëmbejnë ose rrëzojnë aeroplanë duke përdorur armë fizike, mund të kryejnë sulme ndaj avionëve nga toka dhe nga distanca të sigurta. Ekspozimi ndaj rrezikut të sistemeve MTA është i lartë, për shkak të kapacitetit të shtuar të terroristëve dhe ekstremistëve në ditët e sotme për të përdorur teknologjitë e IT dhe atë kibernetike për qëllimet e tyre të paligjshme. Kjo tendencë është në rritje në mbarë botën dhe i atribuohet paqëndrueshmërisë politike dhe sociale në disa rajone të saj apo dhe në zona konflikti.

- ***Aktorët shtetëror***ë, mund të jenë pjesë e modelit të kërcënimit të luftës elektronike, megjithëse tradicionalisht kjo është jashtë fushës së sigurimit të aviacionit civil [26]. Me njohuri të mjaftueshme të sistemeve të zbulimit të ndërhyrjeve dhe burimeve të pakufizuara, është e mundur të anashkalohen kontrollet e besueshmërisë apo mbrojtjet e tepërta edhe në sektorin e MTA. Ekspozimi ndaj rrezikut të sistemeve MTA konsiderohet i lartë dhe varet kryesisht nga rrethanat specifike politike.

3. Masat e sigurisë në MTA

Meqenëse siguria e MTA-ve është komponenti kryesor i sigurisë së aviacionit, ai luan një rol kyç në parandalimin dhe reagimin ndaj kërcënimeve që synojnë të gjitha pjesët e sistemit të aviacionit, duke përfshirë asetet kombëtare dhe ndërkombëtare me vlerë të lartë. Përveç kësaj, siguria e MTA ka një ndërfaqe me Sigurinë e Hapësirës Ajrore që rrotullohet rreth kërkesave të sigurisë kombëtare dhe mbrojtjes, duke ofruar siguri teknologjike dhe ndërveprim midis sistemeve civile dhe atyre ushtarake[27]. Kërcënimet e sigurisë mund të drejtohen ndaj avionëve ose nëpërmjet tyre drejt objektivave në tokë. Dimensioni ndërkombëtar imponon zbatimin uniform dhe efektiv të masave të përshtatshme. MTA duhet të mbështesë sigurinë kombëtare në lidhje me identifikimin e fluturimeve në territorin kombëtar të një shteti dhe organizatave të Mbrojtjes Ajrore duhet t'u sigurohet të gjitha informacionet e MTA-ve që lidhen me veprimtarinë dhe detyrën e tyre[28].

---

[25] Stouffer K, Falco J, Scarfone K (2007) *Udhëzues për sigurinë e sistemeve të kontrollit industrial* (ICS). Rekomanduar. NIST., nr. SP 800–82, pp 1–157

[26] Strohmeier M et al (2016) *Vlerësimi i ndikimit të sigurisë së aviacionit në fuqinë kibernetike*. Konferenca e 8 ndërkombëtare për fuqinë kibernetike të konfliktit kibernetik.

Në përgjithësi, masat e sigurisë në aviacion shtrihen në një sërë disiplinash sigurie. Nuk ka rëndësi nëse aktivi për t'u mbrojtur është një avion, një aeroport, një qendër kontrolli apo një rrjet informacioni, të gjithë elementët e sigurisë zbatohen në një shkallë të caktuar, siç përmendet tashmë në Standardet e Sigurisë (ISO, NIST, ISA) dhe praktikat e rekomanduara[29]. Në tabelën 3 janë përmbledhur këto masa dhe disiplina bazë të sigurisë në sistemet MTA. Ndërsa parimet e mësipërme të sigurisë mund të zbatohen në një shkallë të caktuar efikasiteti, ekziston nevoja për një "vështrim të përgjithshëm/gjithëpërfshirës" që mbulon të gjitha sfidat e sigurisë së aviacionit për të gjitha fazat e transportit ajror, si në tokë ashtu edhe në ajër, që nga hallka më e dobët e zinxhirit e cila mund të këputet. Në mënyrë të veçantë elementi i fundit i sigurisë për vazhdimësinë operacionale synon të trajtojë degradimet e sistemit MTA. Kjo megjithëse mund të përmbledhë më shumë aspekte menaxheriale, është një pjesë thelbësore e ciklit të përgjithshëm të sigurisë së aviacionit. Ai thekson nevojën për prezantimin e një strategjie tërësore të mbrojtjes, parandalimit dhe reagimit.

Disiplina e sigurisë	**Masat e sigurisë**
Siguria fizike	Kontrolli i aksesit, mbrojtja e perimetrit dhe kontrolli i tij, kontrollet e sigurisë, përgjegjësia e aseteve, tepricat, mbrojtja e mjedisit.
Siguria e personelit	Menaxhimi i aksesit të përdoruesve, lejet e sigurisë, ndarja e detyrave, politika e rekrutimit, rregulloret e stafit, verifikimi, ndërgjegjësimi dhe trajnimi i stafit.
Siguria e informacionit	Mbrojtja e informacionit - CIA: konfidencialiteti, disponueshmëria, integriteti; kriptografia, trajtimi i mediave, kopjet rezervë, përditësimet dhe arnimet e softuerit

---

[27] Po aty.

[28] De Zan T, d'Amore F, Di Camillo F - Mbrojtja e sistemeve të trafikut ajror civil nga kërcënimet kibernetike.

[29] https://www.icao.int/Security/SFP/Pages/ SecurityManual.aspx

Siguria e komunikimit	Politikat e ndarjes së rrjetit, menaxhimi i sigurisë, menaxhimi i zbulimit të ndërhyrjeve, regjistrimi i ngjarjeve, puna në telekomandë dhe pajisjet celulare
Mbështetja e inteligjencës	Siguria pa inteligjencë është e pakuptimtë; Mbështetja e inteligjencës është një kërkesë e tërthortë për vlerësimet e kërcënimit, vëzhgimin e kërcënimit dhe deklarimin e niveleve të alarmit të sigurisë.
Shkëmbimi i informacionit të sigurisë	Shkëmbimi i informacionit ndërmjet autoriteteve kombëtare, organizatave të sigurisë dhe inteligjencës dhe menaxherëve të sigurisë së MTA-ve, paralajmërimet e sigurisë, nivelet e kërcënimit dhe alarmit, identifikimi dhe njoftimi i incidentit, raportimi dhe ndjekja e zgjidhjes së incidentit.
Vazhdimësia operative	Reagimi ndaj urgjencës, menaxhimi i vazhdimësisë së biznesit dhe planet e emergjencës nevoja për menaxhimin e elasticitetit.

Tabela nr. 2 - Masat dhe disiplinat bazë të sigurisë në sistemet MTA

4. Rezistenca kibernetike në kontekstin e aviacionit

Ideja e qëndrueshmërisë kibernetike në TIK, në formën e saj më themelore, është vlerësimi i asaj që ndodh përpara, gjatë dhe pasi një sistem i rrjetit digjital përballet me një kërcënim. Rezistenca nuk është specifike për ngjarjet: ajo rritet në një afat të gjatë dhe duhet të përfshihet në strategjinë e përgjithshme të biznesit ose organizimit. Kuptimet e ndryshme të elasticitetit përshkruhen në projektin IMPROVER 1 (është një projekt Horizon 2020 që fokusohet në atë se si të përmirësohet elasticiteti i infrastrukturës kritike evropiane), duke marrë parasysh një kombinim të vetive të ndryshme[30]. Disa përkufizime synojnë largpamësinë, qëndrueshmërinë, shkathtësinë, tepricën, rikuperimin e shpejtë dhe përshtatshmërinë ndërsa disa të tjerët konsiderojnë parandalimin, gatishmërinë, reagimin dhe rimëkëmbjen. Sipas IMPROVER, konceptet e elasticitetit përfshijnë disa dimensione, si ato teknike, organizative, sociale dhe ekonomike, si më poshtë:

Dimensioni teknologjik i referohet kryesisht vetive fizike të komponentëve dhe sistemeve të infrastrukturës dhe i referohet karakteristikave dhe sjelljes së tyre në rastin e një ndryshimi/incidenti.

Dimensioni organizativ, lidhet me organizatat dhe institucionet që menaxhojnë komponentët fizikë të sistemeve, d.m.th., operatorët/pronarët e infrastrukturës kritike. Ai mbulon aspekte të tilla si kultura, njerëzit, vazhdimësia e biznesit, menaxhimi i rrezikut dhe fatkeqësive në nivel organizativ.

---

[30] Theocharidou M et al (2016) D1.3-leksiku përfundimtar i përkufizimeve në lidhje me elasticitetin e infrastrukturës kritike, Kërkimi horizont 2020 i BE.

Dimensioni social përfshin karakteristikat e popullsisë dhe komunitetit që i bëjnë grupet sociale ose më të cenueshme ose më të adaptueshme ndaj rreziqeve dhe fatkeqësive.

Dimensioni ekonomik fokusohet në uljen e drejtpërdrejtë dhe të tërthortë të humbjeve ekonomike që vijnë nga fatkeqësitë, në nivele të ndryshme.

Në kontekstin e aviacionit, programi kërkimor Eurocontrol përdor për elasticitetin përkufizimin e mëposhtëm: “Elasticiteti është aftësia për të parandaluar ndërprerjet, për t’u përgatitur dhe përshtatur ndaj kushteve në ndryshim dhe për t’u përgjigjur dhe rikuperuar me shpejtësi nga ndërprerjet për të siguruar vazhdimësinë e shërbimeve në një nivel të pranueshëm të performances”. Qëllimi i këtij përkufizimi është të arrijë të kuptuarit se kujdesi për elasticitetin është më shumë i lidhur me menaxhimin e rreziqeve sesa me eliminimin e tyre[31]. Të qenit elastik nënkupton minimizimin e reduktimeve (rënie të pranueshme) të performancës përballë një sulmi të suksesshëm. Kjo do të thotë të jesh në gjendje të punosh siç duhet në disa nivele të gjendjes së degraduar, ndërkohë që mund të ndërmerren masa riparimi/“shërimi”. Prandaj është thelbësore të sigurohen metoda dhe mjete për të lejuar që zgjidhja të rikuperohet sa më shpejt që të jetë e mundur nga mënyra të tilla degradimi, sigurisht duke arritur kohën minimale të rikuperimit. Siç paraqitet në fig. 2, nën ombrellën e elasticitetit, i gjithë grupi i masave, të cilat kërkohen për qëndrueshmëri të mjaftueshme ndaj sulmeve kibernetike, është një kombinim i veprimeve të ndryshme dhe sjelljes së duhur para, gjatë dhe pas incidentit[32].

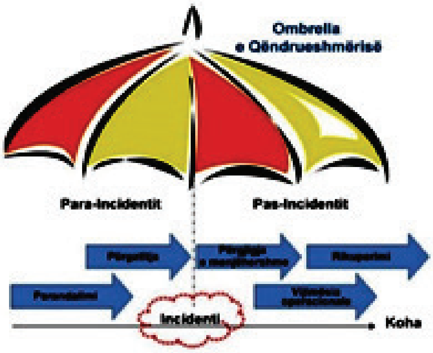


Figura nr. 2. Ombrella e elasticitetit.

Rrjedha e veprimeve të elasticitetit kibernetik fillon tashmë kur shërbimet, mjetet ose sistemet në fjalë janë në fazën e zhvillimit, e cila lidhet me “sigurinë sipas dizajnit”. Kur merret parasysh kjo, hapi i parë është “Parandalimi”. Një tjetër shtyllë e rezistencës është

---

[31] Eurocontrol (2012) Manual për mbikëqyrjen e sigurisë kombëtare të MTA, Publikim i Eurocontrol.

[32] Eurocontrol (2009) Letër e bardhë mbi teknologjinë e rezistencës për MTA. https://www.eurocontrol.int/sites/default/files/article/content/documents/nm/safety/safety-a-white paper-resilience-engineering-for-MTA.pdf

“Përgatitja” për sulme të mundshme, e cila mund të arrihet me procedura dhe trajnime të stafit. Përgatitja për çdo sulm kibernetik fillon me të menduarit për aktivitetet e përditshme dhe mënyrën se si organizohet dhe kryhet puna. Kjo përfshin gjithashtu njohuritë për mënyrat më të shpejta dhe më të sigurta të shkëputjes së mjeteve softuerike nga sistemi ose rrjeti dhe mbylljen e sigurt të sistemeve të infektuara[33].

Kur jeni nën sulm, “Përgjigjja Urgjente” ndaj sulmit është gjithashtu e rëndësishme. Përgjigja fokusohet në identifikimin e problemit, mbajtjen e tij, zhdukjen e tij. Masat reaguese mund të përfshijnë gjithashtu kufizimin e shërbimeve ose zbërthimin e sekuencave të trajnuara. Fokusi do të mbahet në ofrimin e sigurt të shërbimeve dhe të dhënave duke qenë në dijeni të sulmit në vazhdim. Kjo mbështet dhe përmirëson “Vazhdimësinë Operacionale”. Faza e reagimit duhet të vazhdojë derisa shkaku dhe madje edhe efektet kaskaduese të sulmit të jenë eliminuar, llogaritur ose eliminuar gradualisht. Nëse në çdo moment të kohës kjo mund të konfirmohet me siguri, atëherë mund të fillojë faza e “Rimëkëmbjes”. Kjo fazë përsëri duhet të jetë sa më e shkurtër që të jetë e mundur në mënyrë që të gjitha shërbimet, mjetet dhe sistemet të jenë në funksion të plotë pas një sulmi kibernetik.

Megjithëse inxhinieria e elasticitetit është futur në aviacion kryesisht për rritjen e sektorit të sigurisë, ajo nuk është zgjeruar plotësisht në aspektet e sigurisë kibernetike dhe elasticitetin në fushën e menaxhimit të trafikut ajror. Rezistenca në sektorin e aviacionit është diskutuar pjesërisht në kërkimet e mëparshme[34] [35]. Megjithatë ka projekte si ai ARIEL për Rezistencën e Trafikut Ajror, i cili synon të kryej një analizë gjithëpërfshirëse të rrezikut dhe vlerësimin e infrastrukturave kritike në aviacion[36]. Sipas ARIEL, elasticiteti shihet si aftësia e një sistemi për të thithur ose shmangur dëmtimin pa pësuar dështim të plotë dhe integron aspektet e mbrojtjes, zbutjes dhe rikuperimit. Projekti propozon një proces të vazhdueshëm dinamik dhe të bazuar në modele të analizës së rrezikut kibernetik, në mënyrë që të vendosen aftësitë e qëndrueshme të elasticitetit kibernetik në sistemin e transportit ajror.

Projekti ARIEL ka identifikuar disa rekomandime thelbësore (R-), për qëndrueshmërinë në sektorin e aviacionit, të cilat renditen dhe shpjegohen shkurtimisht më poshtë:

---

[33] Eurocontrol (2009) Letër e bardhë mbi teknologjinë e rezistencës për MTA.

[34] Kreuzer M, Kiesling T (2017) Rekomandime për forcimin e qëndrueshmërinë kibernetike të sistemit të trafikut ajror, ARIEL, Qëndrueshmëria e trafikut ajror.

[35] Lykou G, Anagnostopoulou A,Gritzalis D (2018) Zbatimi i masave të sigurisë kibernetike në aeroporte për të përmirësuar qëndrueshmërinë kibernetike, WIIoTS në Samitin e Dytë Global të IoT.

[36] Kreuzer M, Kiesling T (2017) Rekomandime për forcimin e qëndrueshmërinë kibernetike të sistemit të trafikut ajror, ARIEL, Qëndrueshmëria e trafikut ajror.

R-1) Zhvilloni bazën strukturore dhe procedurale për analizën e vazhdueshme të qëndrueshmërisë kibernetike brenda organizatës dhe midis organizatave: Kjo kërkon kombinimin e sigurisë klasike të informacionit dhe qasjeve të reja të elasticitetit operacional kibernetik si dhe krijimin e një strukture organizative që bashkon personelin e të gjitha disiplinave përkatëse brenda dhe mes organizatave të trafikut ajror për të përballuar peizazhin në zhvillim të kërcënimit kibernetik në një mënyrë holistike. Kjo duhet të kombinohet me procese të përshtatshme të vazhdueshme në përputhje me normat e standardet ekzistuese të sigurisë së informacionit.

R-2) Zhvillimi dhe administrimi i ekipeve ndërdisiplinore të analizës së rrezikut kibernetik: Për të lehtësuar krijimin e ekipeve bashkëpunuese ndërdisiplinore, ekziston nevoja për të zhvilluar dhe zbatuar metodat e nevojshme dhe qasjet e menaxhimit që përbëjnë elementë të një gjuhe të përbashkët; menaxhimi dhe transferimi i njohurive; menaxhimin e mungesës së dijeve për vlerësimin e balancuar të gjetjeve; përhapje të njohurive bazë në IT dhe ndërgjegjësim për sigurinë nga personeli i të gjitha disiplinave duke përfshirë menaxhimin e mesëm dhe atë të lartë.

R-3) Zhvillimi dhe mirëmbajtja e një portofoli të skenarëve të kërcënimit kibernetik: Ndryshe nga mënyra e aplikuar aktualisht ad-hoc e zhvillimit dhe përdorimit të skenarit të kërcënimit rekomandohet, prezantimi i një procesi të strukturuar të vazhdueshëm për zhvillimin dhe evoluimin e skenarëve të kërcënimit kibernetik të trafikut ajror. Kjo duhet të kombinohet me metodologjinë e përshtatshme për të zhvilluar skenarë dhe për t'i zbatuar ato në fushat e zhvillimit të njohurive, trajnimit si dhe verifikimit dhe vërtetimit.

R-4) Sigurimi i ndërveprimit të modeleve dhe të dhënave të rëndësishme kibernetike: Nevojitet zhvillimi i meta-modeleve të standardizuara për shkëmbimin e të dhënave të bazuara në kompjuter dhe bashkëpunimi i modeleve të ndryshme. Integrimi dhe krahasimi i rezultateve dhe gjetjeve të rëndësishme për kibernetikën në analizën e bazuar në mjete vlerësohet thelbësor. Për të mundësuar bashkëpunimin ndërdisiplinor apo edhe ndërfushën bazuar në një qasje gjithëpërfshirëse, nevojiten koncepte të shkëmbimit të të dhënave për një ripërdorim të të dhënave ekzistuese, të cilat përfshijnë aspekte teknike, metodologjike dhe organizative.

R-5) Përsosja dhe zhvillimi i metodave të analizës dinamike të rrezikut: Duhet të zhvillohen përpjekje shtesë për vlerësimin dhe zhvillimin e mëtejshëm të metodës së analizës dinamike të rrezikut të bazuar në model. Kjo analizë gjysmë e automatizuar mundëson modelimin dhe analizimin dinamik të rreziqeve kibernetike në sisteme komplekse, organizata të mëdha apo dhe mes disa organizatave të ndërlidhura. Potenciali i lartë i kësaj qasjeje mundëson vlerësim gjithëpërfshirës dhe dinamik të rrezikut kibernetik në sektorin e aviacionit.

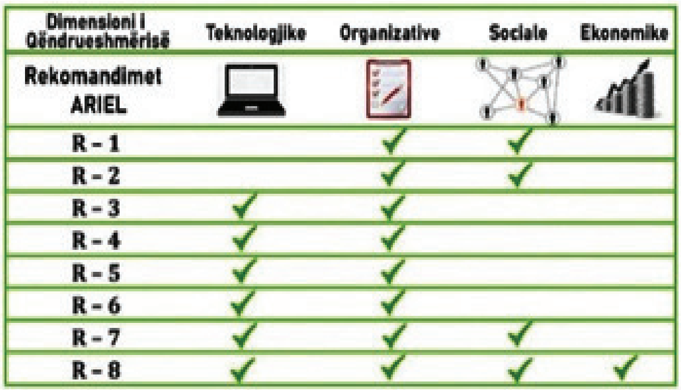
R-6) Mbrojtja dhe siguria: Siguroni qëndrueshmëri dhe mundësoni sinergji meqenëse kërcënimet dhe sulmet e mundshme kibernetike mund të kenë një ndikim të drejtpërdrejtë në funksionet e sistemit kritik për sigurinë. Prandaj, kërkohet zhvillimi i një qasjeje gjithëpërfshirëse të menaxhimit të rrezikut që përafron konsideratat e mbrojtjes dhe sigurisë nën një çati të përbashkët.

R-7) Përmirësimi i metodologjive të projektimit për të siguruar karakteristikat elastike të sistemit gjatë gjithë ciklit të jetës: Ristrukturimi i arkitekturave të sistemeve socio-teknike mund të mbështesë elasticitetin kibernetik përveç masave mbrojtëse. Qasjet ekzistuese të inxhinierisë së elasticitetit, të cilat fokusohen kryesisht në faktorët njerëzorë në sistemet komplekse, duhet të shtrihen në një kuptim teknik drejt integrimit të aftësive të elasticitetit kibernetik. Disa nga aspektet më të rëndësishme që duhen marrë parasysh janë: përgatitja e arkitekturave për ndryshime të vazhdueshme; konsiderimi i strategjive të zbutjes dhe rikuperimit në hartimin e sistemit; dhe shtimi i funksioneve të sistemit që mbështesin zbulimin e sulmeve kibernetike.

R-8) Shfrytëzo metodologjitë e simulimit për të mbështetur kërcënimin kibernetik dhe analizën e rrezikut të sistemeve komplekse: Për të arritur një kuptim gjithëpërfshirës të efekteve të sulmeve të mundshme kibernetike në sistemet komplekse, simulimi është një metodë e vlefshme për të plotësuar metodat më tradicionale të analizës.

Një aplikim i gjerë i modeleve të simulimit për proceset dhe sistemet duhet të identifikohet nga kërcënimet kibernetike dhe analiza e rrezikut për të qenë kritike për funksionimin e sistemit. Simulimi rrit të kuptuarit e ndikimit të kërcënimeve kibernetike të identifikuara dhe mbështet vërtetimin e rezultateve të analizës së rrezikut. Përveç përdorimit të modeleve ekzistuese të simulimit si mjete të pavarura, është e rëndësishme të zhvillohen modele simulimi “nga porta në portë” për të mbështetur analizën gjithëpërfshirëse të proceseve të aviacionit. Së fundi, përdorimi i simulimit është jetik me stafin operacional për të hulumtuar bazat e faktorëve njerëzorë përballë sulmeve të mundshme kibernetike. Bazuar në rekomandimet e ARIEL, janë analizuar dimensionet gjithëpërfshirëse të elasticitetit të cilat, sipas koncepteve të IMPROVER, janë teknike, organizative, sociale dhe ekonomike (rezultatet janë paraqitur në fig. 3).

Ajo që mund të kuptohet nga analiza e tabelës është se shumica e rekomandimeve mbulojnë të paktën dy dimensione të elasticitetit me ato teknologjike dhe organizative që janë më të zakonshmet. Ekziston një ndryshim thelbësor i rekomandimeve të elasticitetit nga disiplinat e sigurisë kibernetike, të cilat zakonisht trajtojnë një dimension të vetëm në të njëjtën kohë. Masat e elasticitetit duket se janë një sintezë e ndërveprimeve, bashkëpunimit dhe evolucionit të qasjeve aktuale të sigurisë kibernetike. Dimensioni organizativ është i përbashkët për të gjitha rekomandimet, pasi elasticiteti kibernetik është vërtetë një çështje e menaxhimit efektiv të rrezikut, e kombinuar me punë bashkëpunuese dhe strategji ndërdisiplinore për të siguruar kontingjent dhe vazhdimësi efikase të biznesit.



Dimensioni i Qëndrueshmërisë	Teknologjike	Organizative	Sociale	Ekonomike
Rekomandimet ARIEL				
R - 1		✓	✓	
R - 2		✓	✓	
R - 3	✓	✓		
R - 4	✓	✓		
R - 5	✓	✓		
R - 6	✓	✓		
R - 7	✓	✓	✓	
R - 8	✓	✓	✓	✓

Figura nr. 3 Dimensioni i qëndrueshmërisë në rekomandimet e ARIEL

Ndërkohë që ka mungesë rekomandimesh që zbatojnë dimensionin ekonomik të qëndrueshmërisë së aviacionit, dimensioni social është gjithashtu më pak i zhvilluar. Rekomandimi i vetëm që mbulon të katër dimensionet e elasticitetit është i fundit, në lidhje me arritjen e një kuptimi të përbashkët/ gjithëpërfshirës të efekteve të sulmeve të mundshme kibernetike me metodologjitë e simulimit të cilat mbështesin më mirë analizën e rrezikut kibernetik të sistemeve komplekse. Për të promovuar një qasje të përgjithshme të qëndrueshmërisë kibernetike në sektorin e aviacionit, strategjia afatgjatë duhet të kombinojë të gjitha dimensionet e elasticitetit që janë teknologjik, organizativ, shoqëror dhe ekonomik. Kjo qasje mund të sigurojë performancë dhe gatishmëri më të madhe, duke i bërë sistemet më efikase dhe efektive.

Përfundime

Qasjet e fundit për të rritur kapacitetin dhe efikasitetin e sistemit ekzistues të trafikut ajror kanë çuar në një përpjekje të madhe të tranzicionit drejt digjitalizimit dhe automatizimit. Si rezultat, sistemet e IT të ndara më parë lidhen nëpërmjet rrjeteve të sapo krijuara për shkëmbim informacioni dhe të dhënash. Për shkak të rritjes së kompleksitetit, sipërfaqja e sulmit të sistemit të përgjithshëm të aviacionit po rritet dhe po krijohen ndërvarësi të panjohura më parë. Kufizimi i menaxhimit të rrezikut të sigurisë në aspektet fizike "tradicionale" si terrorizmi ajror nuk është më i mjaftueshëm për të siguruar një funksionim të qëndrueshëm dhe të fuqishëm të sistemit të transportit ajror. Komponenti i sigurisë kibernetike duhet të zgjerohet nga qasjet tradicionale të zbutjes së rrezikut në qasje më elastike.

Fushat e transportit ajror dhe të sigurisë kibernetike janë të organizuara me fokus të fortë në mekanizmat mbrojtës, përsa i përket zbatimit të tyre operacional dhe teknik. Për të përmbushur kërkesat e përshtatjes së vazhdueshme ndaj një mjedisi kërcënimi që ndryshon me shpejtësi, arkitekturat e sistemeve operative dhe teknike duhet të ristrukturohen bazuar në rezultatet dhe analizën dinamike të simulimit të rrezikut.

Rekomandohet që të balancohet zhvillimi i drejtuar nga kostoja dhe performanca dhe t’i jepet përparësi një përmirësimi të qëndrueshëm, gjithëpërfshirës dhe të vazhdueshëm në mënyrë që të përmirësohet elasticiteti i përgjithshëm i sistemit kibernetik.

Meqenëse siguria dhe ruajtja janë shtytës për përcaktimin e kërkesave për elasticitet, është e arsyeshme të merret një pikëpamje e integruar për të dyja çështjet për të nxitur konsistencën e koncepteve të elasticitetit në aviacion. Meqe elasticiteti kibernetik është vërtetë një çështje e menaxhimit të rrezikut, nuk ka asnjë pikë të vetme në të cilën fillon apo përfundon. Në vend të kësaj, ajo vjen nga ndërtimi i strategjisë dhe nga puna për të siguruar që mekanizmat e transferimit të rrezikut që funksionojnë për kërcënimet më tradicionale, të vihen në zbatim edhe ndaj kërcënimeve të reja kibernetike. Të qenit elastik kërkon që ata që janë në nivelet më të larta të një kompanie, organizate apo qeverie të njohin rëndësinë e shmangies dhe zbutjes së rreziqeve. Ndërsa është përgjegjësi e të gjithëve që të bashkëpunojnë, për të siguruar qëndrueshmëri më të madhe kibernetike, drejtuesit që përcaktojnë strategjinë për një organizatë janë përgjegjësit kryesorë për përfshirjen e qëndrueshmërisë kibernetike në strategjinë organizative.

Bibliografia:

1. Lim B. Siguria e aviacionit-kërcënimet e reja kibernetike në aviacion-sfidat dhe masat zbutëse.
2. Grupi i Nivelit të Lartë të Industrisë (Industry High-Level Group). Raporti i përfitimeve të aviacionit 2017.
3. De Zan T, d’Amore F, Di Camillo F (2015) Mbrojtja e sistemeve të trafikut ajror civil nga kërcënimet kibernetike.
4. Kreuzer M, Kiesling T (2017) Rekomandime për forcimin e qëndrueshmërinë kibernetike të sistemit të trafikut ajror, ARIEL, Qëndrueshmëria e trafikut ajror.
5. Lykou G, Anagnostopoulou A,Gritzalis D (2018) Zbatimi i masave të sigurisë kibernetike në aeroporte për të përmirësuar qëndrueshmërinë kibernetike, WIIoTS në Samitin e Dytë Global të IoT.
6. Strohmeier M et al (2016) Vlerësimi i ndikimit të sigurisë së aviacionit në fuqinë kibernetike. Konferenca e 8 ndërkombëtare për fuqinë

kibernetike të konfliktit kibernetik.

7. Strohmeier M et al. Mbi perceptimin dhe realitetin në sigurinë e komunikimeve të trafikut ajror wireless.
8. Costin A, Francillon A (2012) Fantazma është në ajër (trafiku): mbi pasigurinë e protokollit ADS-B dhe sulmet praktike në pajisjet ADS-B.
9. Organizata Ndërkombëtare e Aviacionit Civil (ICAO) (2013) Aftësia fillestare për mbikëqyrjen tokësore. Në planin global të navigimit ajror 2013–2028.
10. ICAO (2017) Manuali i sigurisë së aviacionit, botimi i 10-të, https://www.icao.int/Security/SFP/Pages/ SecurityManual.aspx
11. CANSO Siguria kibernetike dhe vlerësimi i rrezikut Organ i Shërbimeve të Navigacionit Ajror Civil.
12. Kumar S, Xu B (2017) Vlerësimi i cenueshmërisë për sigurinë në sistemet kibernetike-fizike të aviacionit.
13. Sampigethaya K, Poovendran R, Bushnell L (2008) Funksionimi, kontrolli dhe mirëmbajtja e sigurt e aeroplanëve të ardhshëm, Laboratori i Sigurisë së Rrjetit (Network Security Lab - NSL), Departamenti EE, Universiteti i Washingtonit, Seattle.
14. Lim B (2014) Siguria e aviacionit - kërcënimet e shfaqura nga siguria kibernetike në aviacion – sfidat dhe masat zbutëse, J Aviat Manag
15. Stander A, Ophoff J (2016) Siguria kibernetike në aviacionin civil
16. Jeyakodi D (2015) Siguria kibernetike në aviacionin civil
17. Stouffer K, Falco J, Scarfone K (2007) Udhëzues për sigurinë e sistemeve të kontrollit industrial (ICS). Rekomanduar. NIST., nr. SP 800-82, pp 1-157
18. Theocharidou M et al (2016) D1.3 - leksiku përfundimtar i përkufizimeve në lidhje me elasticitetin e infrastrukturës kritike, Kërkimi horizont 2020 i BE.
19. Lange D et al. Kornizë për zbatimin e koncepteve të elasticitetit ndaj IK. Horizont 2020 i BE
20. Eurocontrol (2012) Manual për mbikëqyrjen e sigurisë kombëtare të MTA, Publikim i Eurocontrol.
21. Eurocontrol (2009) Letër e bardhë mbi teknologjinë e rezistencës për MTA. https://www.eurocontrol.int/sites/default/files/article/content/documents/nm/safety/safety-a-white paper-resilience-engineering-for-MTA.pdf.
22. Delgado L, Cook A, Tanner G, Cristóbal S (2016) Përcaktimi i qëndrueshmërisë në MTA, (proc. i inovacionit SESAR), Universiteti Teknik i Delft, Holandë.

RUBRIKA E DYTË

ANALIZA DHE VLERËSIME PËR SIGURINË DHE MBROJTJEN

Impakti i luftës në Ukrainë në sistemin e mbrojtjes e të sigurisë kombëtare dhe kolektive

Kolonel (R) Msc. Dilaver HOXHA

Trajtesë e shkurtuar.

Ky shkrim shqyrton ndikimin e luftës Rusi-Ukrainë në arkitekturën e mbrojtjes dhe të sigurisë kombëtare dhe globale. Analiza përfshin synimet e palëve, zhvillimet e luftimeve dhe vlerësimet nga ekspertë dhe agjenci të ndryshme.

Studimi thekson rëndësinë e mbrojtjes për anëtarët e NATO-s dhe BE-së, duke u fokusuar në mbështetje për Ukrainën dhe nevojën për rishikimin e politikave dhe strategjive nga këto organizata.

Gjatë gushtit 2024, një sulm ukrainas në Kursk synoi të ushtrojë presion mbi forcat ruse, megjithatë, nuk ndryshoi ndjeshëm situatën në vijën e frontit. Konflikti vazhdon të paraqesë sfida të mëdha dhe komplekse për sistemin e sigurisë kombëtare dhe kolektive.

Fjalët kyçe: lufta në Ukrainë, NATO, siguria kombëtare dhe kolektive, arkitektura e mbrojtjes, ofensiva ushtarake, sanksione, strategjitë e mbështetjes, mësimet e nxjerra, teknologjitë ushtarake, efektet ekonomike globale, zhvillimet teknologjike, sfidat e konfliktit.

1. Zhvillimet kryesore të luftës në Ukrainë

1.1. Shkaku i konfliktit dhe qëllimet e aktorëve kryesorë.

Konflikti mes Rusisë dhe Ukrainës ka përfshirë NATO-n dhe aleatët perëndimorë, të cilët mbështesin Ukrainën. Ndërkohë, disa vende autoritare mbështesin hapur Rusinë ose ruajnë partneritete strategjike me të. Po ashtu, ishin dhe aktorë joshtetërorë si “SpaceX” dhe grupi paramilitar rus “Wagner” të cilët kanë luajtur rol të rëndësishëm.

Shkaku i pushtimit rus në Ukrainë:

Rusia kërkonte të ndalonte Ukrainën nga anëtarësimi në NATO dhe të ruante ndikimin e saj në rajon. Për Rusinë, NATO është një aleancë që mbështet interesat amerikane dhe një zgjerim i saj do të kufizonte ndikimin rus në Ukrainë. Rusia gjithashtu e konsideron Ukrainën si një pjesë të pandashme të historisë dhe kulturës së saj.

Qëllimet kryesore të Rusisë:

- Rikthimin e Ukrainës në sferën e ndikimit rus: Rusia dëshiron të parandalojë anëtarësimin e Ukrainës në NATO dhe BE dhe të lidhë politikën dhe ekonominë e Ukrainës me të sajat.

- Rikthimin e territoreve historikisht të rusëve: Rusia synon të rimarrë territore që u bëjnë pjesë e Ukrainës për shkak të ndarjeve të Bashkimit Sovjetik.

Drejtimet kryesore të pushtimit:

- Ofensiva drejt Kievit: Pjesë e forcave speciale dhe një sulm ajror dhe tokësor për të ndërruar regjimin në Ukrainë, duke ndjekur shembuj nga e kaluara.

- Ofensiva në lindje dhe jug të Ukrainës: Për të kapur territor dhe për të shfrytëzuar kontrollin e Krimesë.

Qëllimet e Ukrainës:

Ukraina synon rikthimin e territoreve të pushtuara dhe mbrojtjen e sovranitetit si një shtet demokratik dhe i pavarur. Strategjia e saj përfshin ofensiva ushtarake dhe përpjekje diplomatike për mbështetje ndërkombëtare dhe rivendosjen e integritetit territorial. Fillimisht, Ukraina kërkonte thjesht mbijetesën dhe ruajtjen e territorit, por disfatat e forcave ruse dhe ngadalësimi i ofensivës i dhanë besim Ukrainës për rikuperimin e territoreve të humbura.

Qëllimet e NATO-s:

NATO mbështet Ukrainën për të arritur synimet e saj dhe ka vendosur sanksione ndaj Rusisë për të ndaluar forcimin e regjimit të Putinit në Ukrainë. Mbështetja përfshin ndihmën në çlirimin e zonave të pushtuara dhe krijimin e kushteve për anëtarësimin e Ukrainës në NATO.

1.2. Përmbledhje mbi rezultatet e luftimeve (shkurt 2022 - gusht 2024).

Më 24 shkurt 2022, Rusia filloi një “Operacion Special Ushtarak” në Ukrainë me trupa që morën pjesë në sulme tokësore, detare dhe ajrore. Forcat ruse u përpoqën të marrin Kievin dhe të godasin udhëheqësit ukrainas, por përballë qëndrueshmërisë së forcave ukrainase, plani i tyre për një fitore të shpejtë dështoi.

Përkundër pritshmërive perëndimore, Ukraina tregoi vitalitet dhe qëndresë. Pas një periudhe të parë të suksesshme, Ukraina humbi një pjesë të territorit, por fitoi përsëri disa zona në vitin 2023. Forcat ruse rifituan disa territore, si qyteti i Bakhmut, por me kosto të lartë. Ndihmat e ngadalësuara dhe problemet në përgatitjen e forcave ukrainase kontribuuan në këtë ndryshim. Pas disfatës së vitit 2022, Rusia rriti mobilizimin dhe prodhimin ushtarak dhe kërkoi ndihmë nga vende si Irani, Koreja e Veriut dhe Kina. Nga fillimi i vitit 2024, Rusia ndaloi për të ndërtuar një front të fortë mbrojtës dhe për të përballuar kundërsulmet ukrainase.

Lufta ka pasur ndikim të gjerë në mbarë botën demokratike dhe studimet e ndryshimeve dhe pasojave të saj nuk ofrojnë një parashikim të qartë për të ardhmen. Realiteti i sotëm paraqet tre grupime kryesore: (1) vendet që mbështesin Ukrainën, (2) vendet që mbështesin Rusinë dhe (3) vendet me qëndrim neutral, të cilat mund të ndikojnë në zhvillimet e ardhshme.

Në samitin e NATO-s të korrikut 2024 në Uashington, Aleanca riafirmoi mbështetje për Ukrainën dhe lançoi iniciativën “Ukraine Compact” për mbështetje ushtarake dhe financiare. Samiti gjithashtu trajtoi zgjerimin e NATO-s, luftën kundër dezinformimit rus, dhe bashkëpunimin me partnerët e Aleancës.

Në gusht 2023, forcat ukrainase realizuan një sulm në Kursk, si pjesë e një ofensivë për të rimarrë territore të pushtuara nga Rusia në lindje të Ukrainës. Ky sulm synonte të ushtrojë presion mbi forcat ruse dhe të ndihmonte në arritjen e objektivave të Ukrainës, por nuk ndryshoi rrënjësisht situatën në vijën e frontit. Rusia vazhdon të përparojë ngadalë në Donbas, duke theksuar kompleksitetin dhe sfidat e konfliktit të gjatë.

2. Mësimet e nxjerra nga zhvillimi i luftimeve të forcave ruse në Ukrainë

Pavarësisht se pas 30 muaj luftimesh situata në Ukrainë mbetet e paqartë dhe e papërcaktuar, deri tani është e vështirë të parashikohet se kush do të jetë fituesi ose humbësi i këtij konflikti. Përderisa lufta është ende aktive, mësimet e identifikuara nuk mund të jenë të qarta deri në përfundimin e saj. Për shkak të mjegullës dhe dezinformimit, kemi mundësi të kufizuara për të parë përmasat e plota të konfliktit. Lufta e tillë është një ndërmarrje kombëtare komplekse, dhe analiza e plotë e të gjitha elementëve të fuqisë kombëtare të përdorura nga Ukraina dhe Rusia mund të kërkojë vite ose dekada.

Megjithatë, ky konflikt ofron mësime të vlefshme për vendet e tjera në përballjen me agresione të mundshme. Nga fillimi i luftës deri tani, janë identifikuar mësime të rëndësishme që duhet të merren parasysh për të shmangur gabime të ngjashme në të ardhmen.

Mësimet e nxjerra në Ukrainë, ndonëse mund të mos jenë unike për Evropën, janë të rëndësishme për të gjitha palët e përfshira dhe për NATO-n e BE-në. Disa nga drejtimet kryesore përfshijnë: rreziqet e llogaritjeve të gabuara në luftime, mangësitë e lidershipit të forcave ruse dhe gabimet logjistike në fazën fillestare të pushtimit, mungesat në unitetin ndërkombëtar, sfidat e përfundimit të konflikteve të zgjatura, rëndësinë strategjike të rrugëve detare dhe rolin e fuqisë tradicionale të zjarrit me bazë tokësore. Këto mësime duhet të nxisin transformime në Forcat e Armatosura, në të gjitha ushtritë e NATO-s, si dhe në forcat e përbashkëta dhe shumëkombëshe. Ato janë kyçe për formulimin e politikave, planeve, strategjive dhe doktrinave ushtarake për të ardhmen.

Vlerësimet do të jenë të rëndësishme në të gjitha nivelet e komandim-kontrollit (politike, strategjike, operacionale dhe taktike) dhe janë të vlefshme edhe për vendet e vogla që mund të kenë ndikim në këtë konflikt dhe konflikte të tjera të mundshme.

2.1. Vlerësime mbi mësimet e nxjerra në nivel politik dhe diplomatik.

Dënimi i agresionit rus dhe mbështetja për Ukrainën. Dënimi i agresionit rus, mbështetja e Ukrainës dhe vendosja e sanksioneve ndaj Rusisë kanë qenë masat kryesore për të dobësuar veprimtarinë agresive të saj. Qëndrimi i bashkuar i OKB-së, BE-së dhe NATO-s në dëshminë e agresionit rus në Ukrainë ka qenë i menjëhershëm. Perëndimi, përfshirë shumicën e vendeve të BE-së dhe NATO-s, ka vendosur një paketë të gjerë sanksionesh ndaj Moskës. Këto përfshijnë ndalimin e transaksioneve me bankën qendrore të Rusisë, ndalimin e investimeve të reja dhe ngrirjen e aseteve të liderëve rusë. Sanksionet e BE-së për kufizimin e blerjeve të gazit dhe naftës ruse kanë ndikuar në uljen e influencës politike të Rusisë në Evropë dhe në izolimin e Moskës nga Evropa.

Mbrojtja e Ukrainës nga pushtimi rus nuk mund të realizohej pa mbështetje ekonomike, humanitare dhe ushtarake. Vendet dhe institucionet anembanë botës, përfshirë vendet anëtare të NATO-s, BE-së, si dhe institucione si Komisioni Evropian dhe Fondi Monetar Ndërkombëtar, kanë ofruar ndihmë të konsiderueshme. Vlen të theksohet se Shtetet e Bashkuara, Mbretëria e Bashkuar dhe Polonia kanë qenë veçanërisht të angazhuara në ndihmën ushtarake për Ukrainën[1].

Kjo luftë ka theksuar rëndësinë e unitetit dhe bashkëpunimit të NATO-s për të adresuar kërcënimet e sigurisë në Evropë. Megjithëse ka pasur hezitime fillestare, komuniteti transatlantik ka treguar një unitet të jashtëzakonshëm në mbështetje të Ukrainës dhe në forcimin e parandalimit kundër Rusisë. Mësimi kryesor është se për të rivendosur një paqe të qëndrueshme, është e nevojshme të adresohen shkaqet rrënjësore të konfliktit, dhe se agresioni ushtarak përballet me rezistencë të ashpër dhe pasoja të rënda.

Efektet e paparashikuara të luftës dhe përgatitjet për një mjedis të ri të sigurisë. Mjedisi i ri gjeopolitik ka ndikuar në vendimmarrjen për investime në shtete jodemokratike dhe me rrezik të lartë. Lufta në Ukrainë ka forcuar angazhimin e Evropës për të rritur shpenzimet e mbrojtjes. Në vitin 2023, dy të tretat e anëtarëve të NATO-s kanë arritur premtimin e Samitit të Uellsit të vitit 2014 për të investuar 2% të PBB-së në mbrojtje, me të paktën 20% të kësaj shume për prokurimin e pajisjeve të reja dhe kërkimin dhe zhvillimin. Megjithatë, mbetet një pyetje nëse prodhuesit e pajisjeve ushtarake mund të përmbushin kërkesat e rritura për armë dhe municione.

Lufta ka përshpejtuar zbatimin e politikave parandaluese të NATO-s dhe ka forcuar vendosjen e saj në Evropën Lindore, Finlandë dhe Suedi, të cilat kanë shfrytëzuar mundësinë për t'u bashkuar me NATO-n. Mbështetja e SHBA-së për NATO-n është forcuar, dhe aleanca po investon në përmirësimin e aftësive mbrojtëse për të forcuar parandalimin kundër Rusisë. Situata e tanishme krijon një ndarje globale të ngjashme me atë të epokës së Luftës së Ftohtë, ku Rusia është në një dizavantazh të madh për shkak të humbjes së kontrollit mbi ish-anëtarët e bllokut sovjetik.

Mësimi është se agresioni ushtarak ka një çmim të rëndë dhe se liderët duhet të jenë të përgatitur për të përballuar një Rusi të ringjallur dhe autoritare.

Diferenca në qëndrimin e NATO-s ndaj luftës dhe pritshmëritë e Ukrainës. NATO ka shprehur gatishmërinë për të mbështetur Ukrainën me fonde dhe pajisje, por ndihma ka qenë e pamjaftueshme për të mposhtur Rusinë. Shkaqet kryesore për këtë janë hezitimi për të provokuar Rusinë dhe kufizimet politike dhe legjislative. Sanksionet e vendosura nga NATO dhe BE kanë ndikuar në ekonominë ruse, por gjithashtu kanë shkaktuar dëme në ekonomitë e anëtarëve të NATO-s, duke lejuar Rusinë të përshtatet dhe të gjejë rrugë alternative përmes vendeve si Kina dhe India.

Në aspektin diplomatik, mësimi është se vendet perëndimore duhet t'i besojnë më shumë në gjykimin e Ukrainës dhe fqinjëve të saj për të ofruar mbështetje të fuqishme pa kufizime të panevojshme dhe për të mbajtur një front të bashkuar. Nënvlerësimi i Ukrainës ose hezitimi në ofrimin e ndihmës mund të dëmtojë përpjekjet kolektive për të mbrojtur sovranitetin e Ukrainës.

---

[1] Antezza et. al., 2022 Grossi & Vakulenko, 2022

Në Samitin e NATO-s të Vilniusit në korrik 2023, pati mosmarrëveshje mbi mbështetjen për anëtarësimin e Ukrainës në NATO, duke nxjerrë në pah ankesat midis Ukrainës dhe Perëndimit. Megjithatë, NATO shfuqizoi «Planin e Veprimit të Anëtarësimit» (MAP) dhe njoftoi një program mbështetës shumëvjeçar për Ukrainën. Samiti i Uashingtonit në korrik 2024 përqendroi vëmendjen në luftën në Ukrainë dhe u pajtua për ndihmë afatgjatë dhe krijimin e një programi për sigurimin e pajisjeve dhe trajnimin e forcave ukrainase.

Mësimi është se diferenca midis qëndrimit të NATO-s dhe pritshmërive të Ukrainës qëndron në ekuilibrin midis mbështetjes ushtarake dhe realiteteve politike të konfliktit.

Dështimet e Rusisë në arritjen e qëllimeve të saj. Liderët rusë, përfshirë presidentin Putin, nënvlerësuan aftësitë ushtarake të Ukrainës dhe unitetin e Perëndimit. Edhe pse Rusia fitoi territore të mëdha në fillim, nuk arriti të përmbushë qëllimin e saj për të eliminuar regjimin ukrainas. Supozimi i gabuar se shumica e popullsisë së Ukrainës do të mbështeste një regjim pro-rus ishte një dështim i madh i inteligjencës që çoi në përdorimin e forcës shumë të vogël për të arritur qëllimet e caktuara.

Ofensivat e hershme ruse në Ukrainën lindore arritën të kapnin territor të konsiderueshëm, por përpjekjet për të përparuar drejt Odesës dështuan. Mësimi është se gabimet e agresionit rus në Ukrainë theksojnë kompleksitetin e luftës moderne dhe rëndësinë e inteligjencës së saktë, si dhe ndikimin e mbështetjes ushtarake ndërkombëtare.

Lufta patriotike në Ukrainë dhe ndikimi i korrupsionit në përpjekjet për anëtarësim në NATO. Lufta në Ukrainë ka theksuar problemet e korrupsionit politik dhe administrativ, që kanë ndikuar në përpjekjet e vendit për anëtarësim në NATO. Pushtimi rus ka përkeqësuar ekonominë dhe ka krijuar një krizë humanitare dhe ekonomike globale. Indeksi i Perceptimit të Korrupsionit (CPI) tregon se korrupsioni në Ukrainë është i përhapur në forma politike dhe burokratike. Korrupsioni politik përfshin devijimin e ndihmës dhe shpërdorimin e fondeve, ndërsa korrupsioni burokratik ndodh në nivele administrative dhe përfshin ryshfetin[2].

Gjatë luftës, janë shpërthyer raste të shumta korrupsioni, duke përfshirë skandalet që çuan në shkarkimin e zyrtarëve të lartë. Në gusht 2023, presidenti Zelenski pezulloi drejtuesit e zyrave të rekrutimit për shkak të mbi njëqind rasteve korrupsioni. Këto zhvillime kanë nxitur përpjekje për të luftuar korrupsionin, por ky fenomen mbetet një sfidë për sigurinë dhe përpjekjet për anëtarësim në NATO. Mësimi është se, ndërsa Ukraina ka bërë përparime, lufta ka theksuar nevojën për reforma të vazhdueshme për të parandaluar që korrupsioni të dëmtojë përpjekjet për anëtarësim në NATO.

---

[2] Transparency International, 2009,page 37

Diferencat në teknologjitë ushtarake të vendeve të NATO-s dhe ndikimi në rezultatet e luftës në Ukrainë. Pritshmëritë për një revolucion të teknologjisë ushtarake në këtë luftë nuk janë realizuar. Përdorimi i teknologjisë së re nga Rusia dhe Ukraina ka treguar se teknologjitë ekzistuese janë më të rëndësishme në këtë konflikt.

NATO-ja ka ofruar mbështetje për Ukrainën me teknologji që i përshtatet situatës së saj, por mbështetja ka qenë e kufizuar dhe shpesh e vonuar, duke ndihmuar Rusinë të rikuperojë territoret e humbura. Vendet e NATO-s kanë bërë marrëveshje për të krijuar koalicione për mbështetje afatgjatë, duke përfshirë armë dhe municione, për nevoja të menjëhershme dhe fusha kritike si aviacioni dhe mbrojtja ajrore[3].

Mësimi është se, ndërsa NATO-ja ka avancuar teknologjinë, efektiviteti i përpjekjeve shpesh është i ndikuar nga vonesat dhe sfidat logjistike. Konflikti shërben si një provë për aftësinë e NATO-s për t'u përshtatur dhe për t'iu përgjigjur nevojave ushtarake që ndryshojnë me shpejtësi. "....Megjithatë, përballë armiqësive të vazhdueshme, është më e rëndësishme të arrihet epërsia teknologjike "këtu dhe tani", e cila u jep një premium inovacioneve që lidhen drejtpërdrejt me situatën në vijën e parë të frontit, sesa vizioneve të largëta të modernizimit[4].

Impakti i luftës në Ukrainë në ekonominë globale. Lufta në Ukrainë ka shkaktuar ndikime të mëdha në ekonominë globale, duke përfshirë rritjen e çmimeve të energjisë dhe shqetësime për sigurinë ushqimore. Reduktimi i furnizimeve me gaz dhe naftë nga Rusia ka rritur çmimet dhe bllokada detare në Detin e Zi ka ndikuar në furnizimet globale të ushqimit. Mësimi është se lufta ka shkaktuar shqetësime të menjëhershme dhe një sërë sfidash ekonomike globale që do të vazhdojnë për vite. Rritja e çmimeve, inflacioni dhe pasiguria ushqimore reflektojnë pasojat e gjera të konfliktit dhe kërkojnë përgjigje të koordinuara ndërkombëtare për të zbutur ndikimet në popullatat dhe ekonomitë e cenueshme.

2.2. Vlerësime në nivel strategjik.

Sigurimi i fitores në Ukrainë si objektiv strategjik global. Rezultatet e luftës në Ukrainë kanë pasur një ndikim të gjerë në aspektin kombëtar dhe ndërkombëtar, duke prekur funksionimin e të drejtës ndërkombëtare dhe ruajtjen e rendit global. Kjo luftë kërkon një vizion strategjik për të arritur tre objektiva kryesorë: (1) rivendosjen e kufijve të Ukrainës në vitin 1991, (2) rindërtimin e vendit për të promovuar integrimin perëndimor dhe (3) mbajtjen e Rusisë përgjegjëse për krimet e luftës.

---

[3] The Defense Contact Group of Ukraine, September 2023.

[4] "How the battlefield is changing in Ukraine", Polityka Insigh, May 2024.

Strategjia për mbështetje ndaj Ukrainës duhet të përfshijë disa aspekte kyçe, si: (1) integrimin e Ukrainës në rendin e sigurisë evropiane, (2) reduktimin e aftësisë së Rusisë për të anashkaluar sanksionet, (3) luftimin e dezinformimit rus, (4) forcimin e demokracisë dhe (5) mbështetje për ekonominë dhe demokracinë e Ukrainës[5].

Ndërkohë, në aspektin operacional, Rusia fillimisht kishte epërsi në det dhe ajër. Megjithatë, Ukraina ka sfiduar këtë epërsi me strategji të mohimit të detit dhe përdorimin e armëve me rreze të gjatë veprimi. Dronët dhe raketat kanë kufizuar efektivitetin e forcave ruse në det dhe ajër.

Zhvillimet teknologjike dhe ndikimi i tyre në sigurimin e posteve komanduese dhe nyjeve logjistike. Zhvillimet teknologjike, si sistemet autonome dhe armët hipersonike, kanë ndryshuar karakterin e luftës. Në Ukrainë, nyjet logjistike dhe postet komanduese shpesh bëhen objekt i sulmeve të shpejta, duke u shkatërruar në më pak se 24 orë. Dronët dhe inteligjenca artificiale janë bërë mjetet kryesore për këtë qëllim[6]. Një rrjet mbështetës fleksibël dhe i mbrojtur është thelbësor për të siguruar furnizime dhe mirëmbajtje të pa ndërprera. Fitorja në një konflikt të gjatë varet nga qëndrueshmëria dhe aftësia për të rigjeneruar fuqinë luftarake më shpejt se kundërshtari. Ndërveprueshmëria dhe integrimi i forcave dhe kapaciteteve të ndryshme do të përmirësojnë efikasitetin dhe qëndrueshmërinë në konfliktet e ardhshme.

Në përfundim, investimet kolektive në infrastrukturë dhe trajnim do të forcojnë mbështetje dhe bashkëpunim ndërkombëtar. Kjo përfshin ndërtimin e kapaciteteve të partnerëve dhe përmirësimin e integrimit për të adresuar sfidat e përbashkëta dhe për të rritur forcën kolektive në fushën e betejës. Disa nga përfundimet kryesore të këtij sulmi janë:

- **Suksesi i kufizuar dhe efekti strategjik:** Suksese në Kursk mund të kenë ndikim të kufizuar në strategjinë e përgjithshme nëse territori i fituar nuk është i qëndrueshëm.
- **Kontrolli i burimeve**: Rusia mund të kompensojë humbjet falë burimeve dhe kapaciteteve strategjike, duke theksuar rëndësinë e menaxhimit të burimeve në një luftë të gjatë.

---

[5] The Center for Strategic and International Studies (CSIS) in Washington, D.C., Benjamin Jensen and Elizabeth Hoffman, Maj 15, 2024

[6] “Theater Sustainment Transformation: Lessons from the Russia-Ukraine War”, By Maj. Gen. Ronald R. Ragin and Maj. Christopher G. Ingram, April 23, 2024

- **Sfidat e mbajtjes së territorit dhe strategjia politike:** Mbajtja dhe ruajtja e territoreve të pushtuara është sfiduese dhe mund të ngarkojë burimet e Ukrainës.
- **Politika dhe negociatat**: Suksesi ushtarak mund të përdoret për të shtuar presion në negociatat me Rusinë, por nëse territori i fituar nuk shfrytëzohet siç pritej, mund të humbet mundësia për përfitime në bisedime.
- **Dilemat strategjike:** Mbajtja e territoreve të reja mund të ndikojë në burimet dhe të krijojë dilema strategjike në menaxhimin e forcave, duke ndikuar në operacionet në zona të tjera si Donbas.

2.3. Vlerësime mbi mësimet e nxjerra në nivel operacional.

Konflikti në Ukrainë ka theksuar rëndësinë e Operacioneve me Shumë Fusha (Multi-Domain Operations/ MDO) për Arritjen e Objektivave Strategjikë dhe rolin e hapësirës në operacionet ushtarake moderne. MDO përfshin përdorimin e kombinuar të aftësive në tokë, det, ajër, hapësirë dhe hapësirë kibernetike për të arritur objektiva strategjikë. Ukraina ka shfrytëzuar këtë qasje për të sfiduar agresionin rus, duke përmirësuar aftësitë e saj në disa fusha kryesore:

a) Fusha Tokësore: Zhvendosja e prioriteteve.

Në vitin e tretë të konfliktit në Ukrainë, aleatët dhe partnerët e Ukrainës po zhvillojnë strategji për të mbështetur Kievin. Deri më 31 janar 2024, më shumë se 118,000 trupa ukrainase janë trajnuar ndërkombëtarisht, duke përfshirë 16,300 ushtarë në bazat e Ushtrisë Amerikane në Gjermani. Këto trajnime përfshijnë përgatitjen në armë të ndryshme dhe mbështetje për formacione dhe artileri. Koalicioni ndërkombëtar për mbështetje të Ukrainës ka krijuar grupe për fushat si forca ajrore, mbrojtja ajrore dhe teknologjia e informacionit. Polonia ka udhëhequr një koalicion të ri për mjetet e blinduara, me synimin për të siguruar platformat dhe municionin e nevojshëm për Ukrainën.

Ndryshimet e mësuara nga ky konflikt po ndikojnë në modernizimin e forcave të armatosura, duke përfshirë zhvillimin e tankeve dhe mjeteve të blinduara dhe rimbushjen e predhave 155 mm. Sistemi i raketave taktike ATACMS dhe dronët kanë luajtur një rol të rëndësishëm në konflikt. Ndërkohë, janë bërë përmirësime në fushën e tankeve dhe mjetet e blinduara, dhe programi *Future Attack Reconnaissance Aircraft* (FARA) është anuluar në favor të zhvillimit të aftësive pa pilot.

Lufta në Ukrainë ka nxjerrë mësime të rëndësishme mbi domosdoshmërinë e përdorimit të teknologjive të avancuara dhe bashkëpunimin ndërkombëtar për të arritur objektivat strategjikë në një konflikt shumëdimensional.

b) Fusha Detare: Dronë, bllokada dhe anije të mbytura.

Gjatë vitit të dytë të luftës në Ukrainë, konflikti në domenin detar ka qenë më i kufizuar, por në muajt e fundit, aktivitetet janë intensifikuar. Ukraina ka demonstruar aftësinë për të përdorur dronë detarë për të goditur rëndë Marinën Ruse, duke fundosur dhe dëmtuar të paktën 20 anije ruse, përfshirë një cisternë në Detin e Zi. Dronët detarë kanë qenë të efektshëm në Detin e Zi për shkak të hapësirës së kufizuar dhe pikave të lehta për t'u monitoruar. Studimet sugjerojnë se Ukraina ka fituar një avantazh asimetrik në përdorimin e dronëve dhe anijeve të vogla pa pilot. Këto taktika mund të aplikohen në zona të ngjashme si Gjiri Persik, por janë më pak të përshtatshme për oqeanin e hapur. SHBA mund të përdorë taktika të ngjashme nëse do të mbrojë Tajvanin nga një pushtim kinez.

Sipas Jerry Hendrix, ish Kapiten i marinës dhe aktualisht bashkëpunëtor i lartë në Institutin Sagamore me bazë në Indianapolis, "lufta në Ukrainë ka sinjalizuar një ndryshim të rëndësishëm në mënyrën se si ne e perceptojmë luftën detare, sepse Ukraina ka demonstruar se ka një avantazh të madh asimetrik në përdorimin e dronëve dhe anijeve të vogla pa pilot, të tilla si Ski Jet me bomba mbi to"[7].

Një aspekt tjetër i rëndësishëm është fuqia shkatërruese e një bllokade detare. Rusia ka përpjekur të bllokojë eksportet e drithërave ukrainase, duke shkaktuar probleme ekonomike dhe sociale, veçanërisht në Afrikë. Kjo ka nxjerrë në pah varësinë e botës nga qasja e papenguar në det. Një marrëveshje ndërkombëtare e vitit 1936 jep Turqisë kontroll të madh mbi Detin e Zi. Hendrix sugjeron se Turqia mund të kishte parandaluar përshkallëzimin e konfliktit nëse kishte lejuar hyrjen e forcave detarë të SHBA dhe aleatëve në Detin e Zi.

c) Fusha Ajrore: Pavarësisht kërkesave nga Kievi, asetet ajrore mbeten të munguar.

Situata ajrore ka ndryshuar pak nga fillimi i luftës. Avionët rusë dhe ukrainas shpesh fluturojnë ulët për të shmangur zbulimin. Megjithatë, Ukraina ka zgjeruar shtrirjen e saj përmes raketave me rreze më të gjatë, si Storm Shadow britanike dhe raketat ATACMS të SHBA, të cilat janë përdorur për të goditur objekte të rëndësishme ruse.

Dronët po përdoren gjithashtu për sulme të ulëta. Aleatët e NATO-s kanë ofruar mbështetje për mbikëqyrjen ajrore dhe po eksplorojnë përdorimin e balonave aerostat. Ukraina po përgatitet të marrë F-16 Fighting Falcons nga disa vende europiane dhe ka nisur trajnimin e pilotëve.

Mësimet e nxjerra nga konflikti në Ukrainë nënvizojnë nevojën për një forcë ushtarake të mirë trajnuar dhe adaptuese, të mbështetur nga teknologjia moderne dhe një logjistikë të fuqishme. Këto mësime do të ndikojnë në zhvillimin e ardhshëm të forcave ushtarake në Evropë dhe më gjerë, duke theksuar rëndësinë e përgatitjes dhe integrimit të teknologjive të avancuara.

---

[7] BREAKING DEFENSE STAFF, on February 23, 2024 https://breakingdefense.com/2024/02/ukraine-war-turns-2-lessons-learned-and-what-comes-next/

2.4. Vlerësime mbi mësimet e nxjerra në nivel taktik.

Mbi bazën e mënyrës si janë zhvilluar luftimet, është konstatuar mungesë në aftësitë profesionale të personelit kryesisht në njohjen e taktikave të këmbësorisë për luftën statike dhe në llogoreve, të cilat kanë dominuar konfliktin. Në këtë aspekt kërkohet të ketë një trajnim më gjithëpërfshirës për këmbësorinë, për të përmirësuar aftësitë taktike dhe për të adresuar dobësitë në fushën e betejës. Ndër mësimet kryesore të nxjerra janë:

- **Taktikat e Lëvizjes të NATO-s**: Në këtë konflikt të llogoreve, taktikat që theksojnë lëvizjen nuk janë aq efektive. Lufta është bërë më statike, më shumë si në Luftën e Parë Botërore, sesa në fushatat moderne të "tronditjes dhe frikës".
- **Aftësitë Taktike të Dobëta**: Shumica e forcave të këmbësorisë ukrainase kanë aftësi të dobëta taktike, për shkak të stërvitjes të kufizuar përpara vendosjes në vijat e para. Kjo ka çuar në situata të rrezikshme, si lëvizjet e ngadalta që mund të lehtësojnë zbulimin nga armiku.
- **Mungesa e Stërvitjeve Bazë**: Taktikat bazë si pastrimi i bunkerëve mungojnë, pasi linjat ruse të llogoreve janë sofistikuar shumë, me rrjete të gjata kalimesh dhe bunkerësh.
- **Përdorimi i Aftësive për Sulme të Fortifikimeve**: Edhe pse taktikat e luftës së afërt mund të mos aplikohen drejtpërdrejt në terrenin rural të Ukrainës, ato janë të dobishme për sulmet ndaj llogoreve dhe fortifikimeve të armikut.
- **Përmirësimi i Stërvitjes Taktike**: Çdo stërvitje taktike, qoftë e rëndësishme apo jo, do të ndihmonte në zhvillimin e një mendësie taktike dhe në zvogëlimin e rreziqeve në vijat e para.

Mësimi kryesor është nevoja për një trajnim të thelluar të këmbësorisë, të fokusuar në realitetet e luftës së llogoreve, për të përmirësuar aftësitë taktike dhe për të zvogëluar dobësitë në fushën e betejës.

2.5. Vlerësime mbi mësimet e nxjerra për vendet e vogla, si Shqipëria.

Ruajtja e aftësive të forta dhe elastike të mbrojtjes kombëtare është thelbësore për vendet e vogla evropiane, si Shqipëria, për të frenuar dhe mbrojtur kundër agresionit nga një kundërshtar më i madh si Rusia. Ndër mësimet kryesore të nxjerra për vendet e vogla janë:

Rëndësia e Luftës Asimetrike: Vendet e vogla nuk mund të fitojnë duke luftuar një luftë konvencionale në kushte të diktuara nga një kundërshtar më të madh dhe më të fuqishëm. Ato duhet të fokusohem në taktikat dhe aftësitë asimetrike për të krijuar dilema për armikun. Kjo përfshin fortifikimin e zonave urbane, shfrytëzimin e teknologjive të avancuara si dronët dhe shmangien e përballjeve të drejtpërdrejta me forcat konvencionale të kundërshtarit.

Nevoja për Thellësi Strategjike dhe Qëndrueshmëri: Vendet që nuk kanë thellësi të konsiderueshme strategjike dhe barriera gjeografike janë të cenueshme ndaj pushtimit të shpejtë nga një fqinj më i madh. Përgatitja e qyteteve dhe infrastrukturës për të qëndruar dhe për t'i rezistuar pushtimit është kritike. Mbajtja e një baze të fortë industriale të mbrojtjes, zinxhirëve të ndryshëm të furnizimit dhe aftësia për të mbështetur një konflikt të zgjatur janë thelbësore për kombet më të vogla evropiane.

Rëndësia e Asistencës së Sigurisë dhe Ndërveprueshmërisë: Ndihma dhe trajnimi ushtarak i jashtëm, si ai dhënë Ukrainës, mund të rrisë ndjeshëm forcën e vendet e vogla që përballen me agresion. Ndërveprueshmëria me aleatët është çelësi. Programet efektive të ndihmës për sigurinë dhe stërvitjet e përbashkëta ndihmojnë në ndërtimin e aftësive dhe qëndrueshmërisë së vendeve partnere.

Në përmbledhje, konflikti në Ukrainë ka treguar se vendet më të vogla duhet të japin përparësi aftësive mbrojtëse asimetrike, të qëndrueshme, elastike dhe të ndërveprueshme për të penguar dhe mbrojtur kundër agresionit të mundshëm nga kundërshtarë më të mëdhenj si Rusia.

3. Disa përfundime për t'u marrë në konsideratë nga eksperienca e luftës për përmirësimin e sistemit kombëtar të mbrojtjes

Ukraina arriti të qëndrojë e fortë ndaj agresionit rus për shumë ditë, javë, muaj dhe vite, përkundër humbjeve të mëdha në personel dhe dëmeve kolosale në mjete luftarake dhe infrastrukturë. Përveç fuqisë patriotike të treguar nga Forcat e Armatosura të Ukrainës, një faktor i rëndësishëm në këtë rezistencë ka qenë mbështetja konstante e NATO-s, BE-së dhe vendeve anëtare dhe partnere, përfshirë Shqipërinë.

Shqipëria ka qenë e angazhuar që në fillim në mbështetje të Ukrainës dhe luftës së saj të drejtë për mbrojtjen e popullit ukrainas. Ajo ka luajtur një rol të rëndësishëm në Këshillin e Sigurimit të OKB-së për të fituar mbështetje diplomatike për Ukrainën dhe ka theksuar nevojën për një veprim efektiv shumëpalësh si metoda më e mirë për zgjidhjen e problemeve të përbashkëta, veçanërisht në fushën e paqes dhe sigurisë.

Siguria dhe mbrojtja kombëtare dhe kolektive lidhen me disa faktorë të rëndësishëm:

1. **Rritja e shpenzimeve të mbrojtjes**: Vendet e NATO-s dhe BE-së pritet të rrisin shpenzimet e mbrojtjes në vitet e ardhshme. Edhe pse ka dallime në shpenzimet e mbrojtjes midis shteteve që janë afër konfliktit dhe atyre që nuk janë, investimet në mbrojtje janë në rritje.
2. **Investimet në sisteme dhe platforma të avancuara të armëve**: Shumë vende të NATO-s dhe BE-së po investojnë në sisteme dhe platformat e avancuara të armëve, duke u përpjekur të adresojnë emergjencën e mbrojtjes kombëtare përmes blerjes së teknologjive dhe pajisjeve të avancuara.
3. **Fragmentarizmi i mbrojtjes evropiane**: Mbrojtja evropiane vlerësohet si e fragmentuar, e cila përbën një problem dhe kërkon shpenzime të përbashkëta për t'u eliminuar. NATO dhe BE duhet të punojnë më shumë në forcimin e politikave të mbrojtjes dhe sigurisë, në hartimin e politikave të reja dhe në rritjen e unitetit ndërmjet vendeve anëtare për të pasur një ndikim më të madh në mbrojtjen e sigurisë dhe paqes.

Përvoja e luftës në Ukrainë ka nxjerrë në pah domosdoshmërinë e zhvillimit të kapaciteteve operacionale për siguri dhe mbrojtje, që mbetet një objektiv kryesor për Aleancën dhe vendet anëtare të saj. Kapacitetet operacionale janë të ndërlidhura me shumë faktorë politikë, ekonomikë dhe teknologjikë, dhe tashmë ekziston një panoramë më e qartë mbi nevojat dhe mundësitë për t'i garantuar ato.

Ndër kapacitetet kryesore që duhet të zhvillohen dhe përmirësohen janë: (1) Kapacitetet e mbrojtjes hibride; (2) Lufta e informacionit; (3) Mbrojtja nga avionët pa pilot; (4) Lufta urbane; (5) Grumbullimi dhe menaxhimi i informacionit; (6) Lëvizshmëria strategjike; (7) Forcat e reagimit të shpejtë; (8) Mbrojtja civile.

Këto kapacitete janë thelbësore për arritjen e suksesit në konflikte të mundshme dhe për përmirësimin e mbrojtjes kombëtare dhe kolektive.

3.1. Ndikimi i luftës në Ukrainë në sigurinë globale.

Lufta e paprovokuar e Rusisë ndaj Ukrainës ka pasur një ndikim të thellë në sigurinë globale, duke dobësuar ndjeshëm stabilitetin ndërkombëtar dhe duke krijuar sfida të reja dhe komplekse për komunitetin ndërkombëtar. Ndikimi i saj ka përfshirë një gamë të gjerë aspektesh të sigurisë globale, ndër të cilat veçohen:

Rritja e tensioneve midis Rusisë dhe Perëndimit: Konflikti ka çuar në një përshkallëzim të tensioneve midis Rusisë dhe vendeve perëndimore (NATO, BE dhe vendet anëtare). Kjo ka përfshirë sanksione ekonomike, manovra ushtarake dhe retorikë të ashpër në nivelet më të larta të drejtimit të palëve respektive.

Kërcënimi bërthamor: Tensionet ekstreme kanë sjellë frikën e një përshkallëzimi bërthamor. Rusia ka përdorur herë pas here retorikën bërthamore dhe ka bërë manovra ushtarake që përfshijnë armë bërthamore, duke rritur shqetësimet për një konflikt të mundshëm.

Ndryshime në marrëdhëniet ndërkombëtare: Lufta ka ndikuar në aleanca dhe partneritete globale, duke shtyrë disa vende të rishikojnë marrëdhëniet e tyre me Rusinë dhe të kërkojnë lidhje të reja strategjike.

Ndryshime në balancën e fuqisë globale dhe roli i aktorëve të tretë: Lufta ka ndikuar në balancën e fuqisë globale, duke sfiduar hegjemoninë perëndimore dhe duke rritur rolin e fuqive të reja si Kina dhe India në arenën ndërkombëtare. Kina, për shembull, ka mbajtur një qëndrim të kujdesshëm, duke ruajtur një balancë midis mbështetjes për Rusinë dhe ruajtjes së marrëdhënieve me Perëndimin.

Sfidat për institucionet ndërkombëtare: Konflikti ka vënë në provë efektivitetin e institucioneve ndërkombëtare si OKB-ja, OSBE-ja dhe Këshilli i Evropës në zgjidhjen e konflikteve dhe ruajtjen e paqes. Këto institucione kanë hasur vështirësi në arritjen e një konsensusi dhe marrjen e masave efektive.

Rritja e bashkëpunimit ushtarak të Perëndimit: Konflikti ka çuar në një rritje të bashkëpunimit ushtarak midis vendeve perëndimore dhe aleatëve të tyre, përfshirë stërvitje të përbashkëta ushtarake dhe ndarjen e inteligjencës.

Ndryshime në politikat e mbrojtjes kolektive dhe sigurisë së vendeve evropiane: Shumë vende evropiane kanë rritur buxhetet e tyre të mbrojtjes dhe kanë rishikuar strategjitë e tyre të sigurisë. NATO gjithashtu ka forcuar praninë e saj në vendet anëtare pranë kufirit me Rusinë.

Rritja e kërcënimeve kibernetike: Lufta ka sjellë një rritje të sulmeve kibernetike, me grupe të lidhura me shtetet që sulmojnë infrastrukturën kritike dhe institucionet qeveritare. Kjo ka theksuar rëndësinë e sigurisë kibernetike në mbrojtjen kombëtare.

Përhapja e armëve dhe materialeve ushtarake: Konflikti ka rritur qarkullimin e armëve dhe materialeve ushtarake në rajon, duke krijuar rrezikun e përhapjes së këtyre armëve në tregjet e zeza dhe te aktorët jo-shtetërorë.

Rritja e nacionalizmit dhe militarizimit: Konflikti ka çuar në rritjen e ndjenjave nacionaliste dhe militarizimit në shumë vende, ndërsa kombet kërkojnë të forcojnë mbrojtjen e tyre kundër kërcënimeve të mundshme.

Kriza e refugjatëve: Lufta ka shkaktuar një valë të madhe refugjatësh, me miliona ukrainas që kanë lënë vendin e tyre për të kërkuar siguri në vendet e tjera evropiane dhe më gjerë. Kjo ka krijuar sfida humanitare dhe logjistike për vendet pritëse.

Ndikimi në tregjet financiare globale: Lufta ka shkaktuar luhatje të mëdha në tregjet financiare globale, duke ndikuar në investime dhe stabilitetin ekonomik. Kjo ka pasur pasoja për ekonomitë në zhvillim dhe për tregjet e ndjeshme ndaj çmimeve të lëndëve të para.

Impakti mjedisor: Konflikti ka pasur pasoja mjedisore, përfshirë ndotjen nga luftimet dhe dëmtimet në infrastrukturën kritike, si centralet bërthamore, që mund të kenë efekte afatgjata mbi mjedisin dhe shëndetin publik.

3.2. Ndikimi i luftës në Ukrainë në sigurinë tonë kombëtare.

Ndikimet e luftës së Rusisë në Ukrainë kanë pasur efekte të thella dhe të shumanshme edhe për Shqipërinë, duke prekur sektorë të ndryshëm dhe duke sjellë sfida dhe mundësi të reja për vendin. Ndikimet kryesore janë:

Shqetësimet e sigurisë: Lufta ka dobësuar sigurinë ndërkombëtare, duke sfiduar rendin e sigurisë globale, përfshirë sigurinë tonë kombëtare si aleat i drejtpërdrejtë i NATO-s. Ekzistojnë shqetësime për mundësinë e përgjigjeve më të sigurta nga Rusia në rajone si Atlantiku Jugor, që mund të kërcënojnë stabilitetin e Shqipërisë.

Marrëdhëniet diplomatike: Shqipëria ka dënuar ashpër agresionin e Rusisë kundër Ukrainës dhe është rreshtuar me Perëndimin për të kundërshtuar pushtimin. Shqipëria ka mbajtur një qëndrim të fortë mbështetës ndaj Ukrainës, duke iu bashkuar sanksioneve të vendosura nga Bashkimi Evropian dhe SHBA kundër Rusisë. Kjo ka forcuar marrëdhëniet e Shqipërisë me aleatët perëndimorë, por gjithashtu ka ndikuar në marrëdhëniet me Rusinë.

Bashkëpunimi ushtarak dhe anëtarësimi në NATO: Lufta ka përforcuar angazhimin e Shqipërisë ndaj NATO-s dhe bashkëpunimin me aleatët e saj. Shqipëria ka marrë pjesë në stërvitje të përbashkëta ushtarake dhe ka rritur buxhetin e mbrojtjes për të përmbushur angazhimet e saj ndaj aleancës.

Roli në organizatat ndërkombëtare: Shqipëria, si anëtare e organizatave ndërkombëtare si OKB-ja dhe OSBE-ja, ka pasur mundësinë të kontribuojë në diskutimet dhe vendimmarrjet për zgjidhjen e konfliktit dhe ndihmën për Ukrainën. Kjo ka përforcuar profilin e Shqipërisë si një aktor aktiv dhe përgjegjës në skenën ndërkombëtare.

Siguria kibernetike: Rritja e kërcënimeve kibernetike lidhur me luftën në Ukrainë ka nxitur Shqipërinë të forcojë masat e sigurisë kibernetike për të mbrojtur infrastrukturën kritike dhe institucionet qeveritare nga sulmet e mundshme.

Ndihma humanitare, migrantët dhe mbështetja ndërkombëtare: Shqipëria ka rritur përfshirjen e saj në ndihmën humanitare për Ukrainën, duke treguar solidaritet përmes ndihmave financiare dhe pranimit të refugjatëve. Vendi ynë gjithashtu ka dërguar pajisje ushtarake në Ukrainë për të mbështetur mbrojtjen e saj kundër pushtimit rus. Kjo ka rritur imazhin dhe ka përmirësuar reputacionin e Shqipërisë në arenën ndërkombëtare, duke forcuar lidhjet me vendet e tjera që mbështesin Ukrainën.

Rritja e ndërgjegjësimit për mbrojtjen civile: Lufta ka rritur ndërgjegjësimin për rëndësinë e mbrojtjes civile dhe gatishmërinë për emergjenca. Institucionet shqiptare kanë forcuar programet dhe politikat për të përmirësuar reagimin ndaj emergjencave dhe krizave.

Politika e brendshme: Kriza ka nxitur diskutime të reja për politikën e brendshme, përfshirë nevojën për reforma ekonomike dhe diversifikimin e burimeve të energjisë. Qeveria është përballur me sfida të reja në menaxhimin e situatës dhe në sigurimin e stabilitetit ekonomik dhe social.

Ekonomia: Shqipëria ka ndjerë ndikimin ekonomik të luftës, kryesisht përmes rritjes së çmimeve të energjisë, karburanteve dhe ushqimeve. Këto ndryshime kanë sjellë inflacion të lartë dhe kanë prekur fuqinë blerëse të qytetarëve. Shqipëria është shumë e varur nga importet e materialeve jetike, si drithërat dhe vaji, nga vendet e përfshira në konflikt.

Turizmi: Konflikti ka ndikuar në flukset e turizmit, me disa turistë që shmangin Evropën Lindore dhe preferojnë destinacione më të sigurta, si Shqipëria. Kjo ka sjellë disa përfitime ekonomike për sektorin turistik të vendit.

Transporti dhe tregtia: Lufta ka ndërprerë disa rrugë tregtare dhe ka ndikuar në koston e transportit ndërkombëtar. Kjo ka pasur një efekt domino mbi çmimet e mallrave të importuara dhe eksporteve, duke ndikuar negativisht në bilancin tregtar të Shqipërisë.

Investimet e huaja: Pasiguria globale dhe tensionet gjeopolitike kanë ndikuar në vendimet për investimet e huaja direkte në Shqipëri. Disa investitorë mund të jenë më të kujdesshëm në këtë periudhë, duke shtyrë planet e tyre të investimeve për shkak të pasigurisë dhe tensioneve.

Rekomandime

Forcimi i bashkëpunimit me vendet aleate: Forcimi i bashkëpunimit me vendet aleate është kyç për rritjen e kapaciteteve operacionale. Pjesëmarrja aktive në stërvitjet e përbashkëta dhe sigurimi i kapaciteteve operacionale të deklaruara në NATO janë të nevojshme për të mundësuar ndërveprimin e forcave në të gjitha llojet e situatave.

Konsolidimi i FARSH: Vijimi i konsolidimit të Forcave të Armatosura të Republikës së Shqipërisë (FARSH) si elementi kryesor i sigurisë dhe mbrojtjes kombëtare është i rëndësishëm. Ky konsolidim duhet të përfshijë:

✓ ***Riformulimin dhe p*ërshtatjen e *publikimeve doktrinare**: Përditësimi* *i dokumenteve dhe strategjive për të qenë në përputhje me politikat, strategjitë dhe standardet kombëtare dhe ato të NATO-s.*

- ✓ ***Plotësimin e strukturave me personel dhe programe trajnimi**: Sigurimi i përputhshmërisë me organikën dhe zhvillimi i programeve bashkëkohore për edukim, trajnim dhe stërvitje.*
- ✓ ***Zhvillimin e programeve të modernizimit**: Investimi në armatime, sisteme, pajisje dhe mjete bashkëkohore dhe të ndërveprueshme* për FARSH.
- ✓ ***Sigurimin e aftësive të plota operacionale**: Në lidhje me njësitë e reja organizative si regjimentet e këmbësorisë, njësitë kibernetike, forcat rezerviste dhe struktura të tjera të nevojshme.*
- ✓ ***Vlerësimin e futjes së shërbimit të detyrueshëm**: Përgatitja e koncepteve, politikave, doktrinave, procedurave të veprimit dhe programeve të trajnimit për të siguruar aftësitë e plota vepruese.*

Riorganizimi/Rivitalizimi i industrisë ushtarake: Përshtatja e industrisë ushtarake me standardet kombëtare dhe të NATO-s si dhe me zhvillimet teknologjike bashkëkohore të vendeve aleate për të garantuar mbështetje efektive për kapacitetet operacionale.

Evidentimi i infrastrukturës kritike: Identifikimi i të gjithë infrastrukturës kritike dhe zbatimi i një strategjie të qartë për të siguruar ruajtjen dhe mbrojtjen e saj në të gjitha llojet e situatave.

Zhvillimi i kapaciteteve të sigurisë kibernetike: Investimi në përmirësimin e kapaciteteve të sigurisë kibernetike për të mbrojtur infrastrukturën kritike dhe informacionin ndjeshëm nga sulmet kibernetike.

Krijimi i politikave të sigurisë energjetike: Zhvillimi i politikave për diversifikimin e burimeve të energjisë dhe përmirësimin e kapacitetit të menaxhimit të krizave energjetike për të minimizuar varësinë nga burime të jashtme.

Inkurajimi i bashkëpunimit me institucione akademike dhe kërkimore: Nxitja e bashkëpunimit me universitetet dhe institucionet kërkimore për të zhvilluar dhe implementuar teknologji dhe inovacione që mund të kontribuojnë në forcimin e mbrojtjes dhe sigurisë kombëtare.

Përmirësimi i komunikimit dhe koordinimit të sigurisë: Forcimi i mekanizmave të komunikimit dhe koordinimit midis institucioneve të ndryshme për të siguruar një përgjigje të shpejtë dhe të koordinuar ndaj kërcënimeve dhe krizave të mundshme.

Bibliografia

1. Two Years in, Russia’s War on Ukraine Continues to Pose Threat to Global Security Ted Crous 2023
2. Under-Secretary-General Rosemary A. Dicarlo’s Remarks to the security council on maintenance of peace and security of Ukraine. New York, 23 June 2023
3. Ukraine war: What are the impacts on the world today? August 23, 2022
4. What are the global security implications of Russia’s invasion of Ukraine? JUN 15, 2022 AMBY PHIL CICIORA |
5. The Russia-Ukraine War’s Implications for Global Security: A First Multi-issue Analysis. Thomas Greminger and Tobias Vestner, August 2022
6. Ukraine War: Toward a New Global Security Order, WRITTEN BY Matteo Frigoli and Maurizio Martellini Submitted: 11 October 2022 Reviewed: 08 November 2022 Published: 15 December 2022.
7. Seven ways Russia’s war on Ukraine has changed the world, Stuart Coles- 2023
8. The geopolitical impact of the conflict in Ukraine Five trends to help businesses manage the potential risks to global security and prosperity. Stefano Moritsch Global Geopolitics Lead KPMG International
9. How the Ukraine war deepens divisions across the Balkans, By Gaetano Massara On Apr 28, 2022.
10. Antezza et. al., 2022 Grossi & Vakulenko, 2022
11. Transparency International, 2009,page 37
12. Javier Cifuentes-Faura works in the Department of Financial Economics and Accounting at the University of Murcia, Spain, 06 January 2024: https://doi.org/10.1002/pa.2905
13. The Defense Contact Group of Ukraine, September 2023.
14. “How the battlefield is changing in Ukraine”, Polityka Insigh, May 2024.
15. The Center for Strategic and International Studies (CSIS) in Washington, D.C., Benjamin Jensen and Elizabeth Hoffman, Maj 15, 2024.
16. “Theater Sustainment Transformation: Lessons from the Russia-Ukraine War”, By Maj. Gen. Ronald R. Ragin and Maj. Christopher G. Ingram, April 23, 2024.
17. International Armoured Vehicles Conference 2024, on June 25-26, 2024 in Austin, TX, United States.
18. BREAKING DEFENSE STAFF, on February 23, 2024. Shih: https://breakingdefense.com/2024/02/ukraine-war-turns-2-lessons-learned-and-what-comes-next/
19. Pasojat ekonomike të luftës në Ukrainë dhe ndikimi në agjendën e integrimit të Shqipërisë në BE. Herlina Muça, qershor 2022.

Shërbimet e Inteligjencës të PMC[1] dhe PSC[2], kërcënimi kryesor hibrid rus për Ballkanin Perëndimor

Dr. Drizan SHALA
Lektor në Universitetin e Sarajevës

Trajtesë e shkurtuar. *Në këtë punim dua të sjell ekspertizën time të grumbulluar gjatë studimeve të mia, si dhe nga hulumtimet e burimeve zyrtare, në lidhje me transformimet që po ndodhin në shërbimet inteligjente të epokës së inteligjencës artificiale. Për arsye të digjitalizimit të hapësirës botërore dhe nevojës për informacione parandaluese të sigurisë, shërbimet inteligjente kanë evoluar në burime njerëzore profesioniste, ligjshmëri dhe në përsosje teknologjike të lartë.*

Zhvillimet gjeopolitike nga njëra anë dhe revolucioni teknologjik i ditëve të sotme nga ana tjetër kanë transformuar shërbimet inteligjente, nga instrumente ligjore të sigurisë kombëtare dhe ndërkombëtare, drejt strukturave të sigurisë private dhe një biznesi fitimprurës, të pakontrollueshëm, në duar të liderëve totalitarë dhe qëllimeve të tyre.

Kompanitë ushtarake private (Private Military Companies - PMC), në ditët e sotme, përveç aksioneve të fshehta dhe sabotimit ushtarak, po furnizojnë gjithnjë e më shumë, me produkte informative, qeveritë, oligarkët dhe korporatat në fushën e spiunazhit industrial.

---

[1] PMC - Private military companies

[2] PSC - Private security companies

Këto shërbime inteligjente private (PSC) rrezikojnë ta futin inteligjencën institucionale në një pikë gjysmë të errët, larg nga kontrolli, llogaridhënia dhe mbikëqyrja e nevojshme demokratike. Risi e viteve të fundit është gërshetimi dhe ngritja e inteligjencës në kompanitë private ushtarake, si industri e cila përfshin si aktet individuale të mercenarizmit, ashtu edhe spiunazhin korporativ, i cili është shumë i avancuar, i mirëpaguar dhe i legjitimuar në shumicën e shteteve.

Në punimin tim dua të asistoj lexuesin ushtarak jo vetëm me informacion njohës dhe profesional, lidhur me këtë fenomen të ri dhe sfidues, por gjithashtu edhe të paralajmëroj për rreziqet dhe kërcënimet në fushën e sigurisë e të mbrojtjes. Përdorimi i "ushtrive pa flamur" bëhet me qëllim që të shmanget përgjegjësia shtetërore e shtetit sponsor të tyre, përballë të drejtës ndërkombëtare për krime lufte.

Fjalët kyçe: Kontraktor Privat Ushtarak (PMC), shërbime inteligjente, mercenar, ushtri private, inteligjencë e korporatës, Kontraktor Privat i Sigurisë (PSC) etj.

1. Shërbimet e inteligjencës dhe përfshirja e tyre brenda kompanive private ushtarake

Shërbimet inteligjente, gjatë luftërave të zhvilluara në shekullin e 19-të, nuk kanë përdorur shumë kompani apo industrinë private të sigurimit, sikur në fillim shekullin e 20-të, ku ushtritë private apo kompanitë private të sigurimit kanë vendin e tyre në avancimin e interesave të atyre shteteve mbrapa të cilave veprojnë shërbimet inteligjente me këto ushtri private/kompani private apo qysh quhen PMC/PSC.

Qeveritë kanë rekrutuar qytetarët e tyre për të siguruar qytetarinë dhe sovranitetin e tyre nga të brendshëm dhe të jashtëm kërcënimet. Qytetarët bënin luftëra në emër të shtetit, për besnikëri, kombësi dhe ideologji. Ky kapacitet për ofrimin e sigurisë brenda dhe jashtë vendit ka çuar në aftësinë e shteteve për të kontribuar në sigurinë kolektive në shkallë rajonale dhe globale.

Grupet terroriste, forcat e kartelit të drogës, etnikisht dhe grupet e armatosura të motivuara nga prirjet fetare, ose ndërmarrjet kriminale të organizuara ndërkombëtarisht janë shembuj të tjerë të privatizimit të konfliktit, ndërsa përdorimi i shtuar i kontraktorëve ushtarakë privatë/kompanive të sigurimit private është një manifestim i privatizimit dhe komercializimit të luftës.

Luftërat e fundit në Bosnje, Sierra Leone, Kosovë, Afganistan dhe Irak u zhvilluan të gjitha me ndihmën e kontraktorëve ushtarakë privatë. Prandaj, mercenarët, siç njiheshin dikur, po lulëzojnë – vetëm tani ata quhen Kontraktorë Ushtarakë Privatë (PMC) dhe Kompanitë Private të Sigurisë (PSC) dhe që janë shpërfaqur si çelës kryesor strategjik të invazionit ushtarak në Ukrainë. Pra, PMC/PSC-të janë kompani private që specializohen në aftësitë ushtarake, duke përfshirë operacionet luftarake, planifikimin strategjik, mbledhjen e inteligjencës, mbështetjen operacionale, logjistikën, trajnimin, prokurimin dhe mirëmbajtjen e armëve dhe pajisjeve. Rritja e industrisë PMC/PSC pasqyron fytyrën e re të biznesit të luftës, duke përfaqësuar shtesën më të re në hapësirën moderne të betejës. Roli i PMC/PSC-ve në luftën bashkëkohore po bëhet gjithnjë e më i rëndësishëm, duke ndryshuar forcat e armatosura në mbarë botën dhe mënyrat si bëhen luftëra.

2. Sfidat e sigurisë në Ballkanin Perëndimor nën kërcënimin e PMC/PSC

Ballkani Perëndimor përballet me një kërcënim shumëplanësh nga Rusia, qoftë nëpërmjet aleatëve të saj në rajon, qoftë nëpërmjet kërcënimeve hibride që vijnë nga vetë Rusia.[3] Gjetjet e deritanishme tregojnë se ambiciet e Rusisë, pas ndërhyrjes në vendet e Ballkanit Perëndimor, janë të drejtuara në mënyrë specifike drejt krijimit të problemeve për BE-në dhe NATO-n.[4] Ato mund të kategorizohen si: gjeostrategjike, perandorake/ideologjike dhe gjeopolitike.

Së pari, ambicia gjeostrategjike demonstrohet nga përpjekja e Rusisë për të parandaluar ose dëmtuar praninë e NATO-s dhe BE-së në rajon, siç ishte rasti në Malin e Zi me përpjekjen për të hyrë në Portin e Tivarit. Rusia do të donte ta përdorte Malin e Zi si shpatë brenda barkut të NATO-s. Së dyti, oreksi perandorak i Rusisë ishte diçka që shumë të intervistuar e theksuan. Siç po tregon lufta në Ukrainë, Rusia nuk hoqi dorë kurrë nga ambiciet e saj perandorake. Ajo e sheh veten si një aktor të fuqishëm gjeopolitik – si në shekujt e mëparshëm – jo vetëm në Ballkan, por edhe në nivel global.[5] Së treti, ambicia gjeopolitike.

Për këtë, bashkëpunimi ndërmjet formacioneve paraushtarake ruse dhe ballkanike ka një histori të gjatë. Qindra vullnetarë rusë luftuan përkrah serbëve gjatë luftërave jugosllave në vitet 1990. Në vitet 2010, vullnetarët serbë iu kundërpërgjigjën, duke iu bashkuar radhëve ruse në Donbas dhe Siri. Gjatë viteve të fundit, nuk ka pasur mungesë të raporteve se Moska po kultivon grupe paraushtarake ballkanike për të sabotuar integrimin e rajonit me institucionet perëndimore. Në vitin 2016, oficerët e inteligjencës ruse në bashkëpunim me radikalët serbë (kontraktorët privatë ushtarakë - Wagner) kryen një grusht shteti të dështuar në Mal të Zi në një përpjekje për të parandaluar anëtarësimin e vendit në NATO.

---

[3] https://balkaninsight.com/2024/05/09/win-win-game-western-balkans-should-up-arms-flows-to-ukraine/

[4] https://library.fes.de/pdf-files/bueros/kosovo/20922-20240122.pdf

[5] Po aty.

Në vitin 2018, Rusia u akuzua për trajnimin e formacioneve paraushtarake për liderin nacionalist të serbëve të Bosnjës, Milorad Dodik dhe raportet u konfirmuan nga ministri i sigurisë i Bosnje-Hercegovinës. Në Serbi, radikalët me lidhje të njohura me Rusinë organizojnë protesta nacionaliste sa herë që udhëheqja serbe intensifikon dialogun me Kosovën: përleshjet më të fundit me policinë ndodhën këtë shkurt. Në fund të vitit 2022, lidhjet e Wagner-it me Ballkanin u bënë tituj ndërkombëtarë kur dy radikalë serbë vizituan selinë e kompanisë në Shën Petersburg, duke nxitur frikën se Wagner synonte të hapte një zyrë rekrutimi në Serbi. Këto frika u nxitën më tej nga një artikull reklamues i punës me Wagner-in, botuar nga RT Balkan, një degë serbe e themeluar së fundmi e Holdingut të propagandës ruse RT.[6] Aktualisht, një sistem i gjerë prej 37 PMC operon në 34 vende, 67% (25) e të gjitha kompanive operojnë në Ukrainë, nga të cilat pothuajse gjysma (12) janë krijuar dhe përdorur ekskluzivisht për të marrë pjesë në armiqësitë në Ukrainë, shihni "vendet në të cilat operojnë PMC-të ruse" në të vërtetë[7].

Por bazuar në informacionet përkatëse nga burime brenda aktorëve të sigurisë në nivel të Brukselit, mund të thuhet se Serbia është aktualisht baza kryesore për të ndikuar në një modus operandi të PMC/PSC që bazohet kryesisht në: *mbledhjen e informacionit të inteligjencës dhe analizimin e tyre, ofrimin e trajnimeve në fushën ushtarake, si dhe krijimin e lidhjeve të forta me grupe të ndryshme interesi që janë kryesisht veteranë të luftërave të fundit ballkanike të viteve '90.* Pra, në Serbi ka operuar zyrtarisht një nga kompanitë ushtarake private ruse, e cila është E.N.O.T., por në bazë të hulumtimit mund të themi se tani vetëm emri entitet ka ndryshuar në EBSSA, e cila ka trashëguar të gjithë infrastrukturën e kompanisë së mëparshme të E.N.O.T.[8] Por ka një rritje të formës së heshtur përmes përdorimit të elementeve kulturore si kampi veror "Zlatibor" në Serbi dhe atij politik përmes elementeve të inteligjencës ruse brenda kontureve malinje të strukturave inteligjente serbe duke bërë të pamundur kontrollin institucional të tyre.

3. Kuptimi dhe përkufizimi i Kompanive Private Ushtarake (PMC) dhe atyre Private të Sigurisë (PSC)

Përkufizimi në terma juridikë dhe ushtarakë të Kompanive Private Ushtarake (PMC) është thelbësor në kontekstin e strategjive moderne ushtarake. PMC/PSC e parë moderne u themelua nga një grup ish-veteranësh të SAS, nën udhëheqjen e Sir David Stirling dhe John Woodhouse, Watch Guard International, në vitin 1965 që mund të kontraktohej për qëllime sigurie dhe ushtarake.[9]

---

[6] https://carnegieendowment.org/russia-eurasia/politika/2023/04/whats-behind-the-posturing-of-russian-mercenaries-in-the-balkans?lang=en

[7] https://molfar.com/en/blog/catalog-of-russian-pmcs

[8] https://jamestown.org/program/russian-pmcs-war-veterans-running-patriotic-youth-camps-in-the-balkans-part-one/

Detyra e parë e kompanisë ishte të shkonte në Jemen për të raportuar mbi gjendjen e forcave mbretërore kur u shpall një armëpushim. Kompania operoi përfundimisht në Zambia dhe Sierra Leone, duke ofruar ekipe trajnimi dhe këshilla për çështjet e sigurisë. Kompania gjithashtu shiste armë dhe personel ushtarak në vende të tjera për operacione të ndryshme të privatizuara. Sir David Stirling gjithashtu themeloi KAS International dhe bashkëpunoi me Fondin Botëror të Natyrës për të reduktuar me forcë gjuetinë e paligjshme dhe kontrabandën e paligjshme të dhëmbëve të elefantit në vende të ndryshme të Afrikës Jugore. Në kohët mesjetare, mercenarët përdoreshin nga mbretërit për të luftuar, por rritja aktuale e mercenarëve ndodhi pas Luftës së Dytë Botërore.

Rritja dramatike në numrin dhe madhësinë e PMC/PSC-ve ndodhi në fund të Luftës së Ftohtë. Lufta e Ftohtë u pasua nga shpërthimi i shumë luftërave të vogla, veçanërisht në Afrikë, ku një numër PMC/PSC, duke përfshirë Sand Line International (MB) dhe Executive Outcomes (Afrika e Jugut), bënë emër.[10] PMC/PSC-të janë entitete joshtetërore që ofrojnë shërbime ushtarake për përfitime financiare, shpesh duke operuar në zona konflikti në mbarë botën. Këto kompani ofrojnë një sërë shërbimesh, duke përfshirë operacione luftarake, mbështetje logjistike dhe trajnime, të cilat mund të plotësojnë apo edhe zëvendësojnë forcat tradicionale ushtarake.

Vitet e fundit, përdorimi i PMC/PSC-ve nga fuqitë e mëdha si SHBA dhe Rusia ka ngritur shqetësime për përgjegjshmërinë, transparencën dhe mjegullimin e linjave midis interesave shtetërore dhe private. Ndërsa shtetet vazhdojnë të mbështeten te PMC/PSC-të për detyra të ndryshme ushtarake, është thelbësore të shqyrtohet ndikimi i këtyre subjekteve në sigurinë ndërkombëtare dhe implikimet për strukturën globale të fuqisë në zhvillim. Në rrethana të tilla, përdorimi i kompanive private të sigurisë ushtarake dhe atyre të sigurisë private mund të shfaqet në terma të shkurtra, pozitivë, veçanërisht në drejtim të përmirësimit të aftësive profesionale të vendit, madje ndonjëherë edhe në drejtim të rritjes së vetëbesimit.[11]

Megjithatë, ndikimi negativ në procesin e demokratizimit mund të jetë i lartë dhe i shumanshëm, veçanërisht nëse shteti nuk ka ndërtuar një mekanizëm për monitorimin e kompanive private të sigurisë dhe ushtarake.[12]

---

[9] Javaid, A. (2021, Jul 6). *jagranjosh*. Retrieved from jagranjosh: https://www.jagranjosh.com/general-knowledge/private-military-company-pmc-and-its-working-1625585527-1

[10] Po aty.

[11] Po aty.

[12] Armin, K. (2007, August 10). *researchgate.* Retrieved from researchgate:https://www.researchgate.net/publication/349325583_PRIVATNA_SIGURNOST

4. Klasifikimet, veçoritë dhe karakteristikat e PMC/PSC

- Mbështetja ushtarake synon të ofrojë mbështetje teknike për klientët e tyre. Ata nuk do të marrin pjesë drejtpërdrejt në planifikimin, ekzekutimin etj., të operacioneve ushtarake por vetëm me logjistikë dhe stërvitje.

- Konsulencat ushtarake janë llojet më të zakonshme të PMC-ve dhe ofrojnë trajnime, planifikim operacional, organizim të forcave të armatosura, etj., për klientët e tyre.

- Ofrues ushtarakë punësohen për të luftuar beteja aktive në emër të klientëve të tyre. Ata luajnë një rol humanitar gjatë konfliktit, nëse kërkohet nga klientët.

Dallimi midis këtyre tre kategorive dhe kontraktorëve të rregullt ushtarakë është se ata janë ofrues shërbimesh, jo prodhues. Në ndryshim nga ndërtimi i tankeve, avionëve, anijeve ose raketave, ata ofrojnë roje të armatosur, këshilltarë ushtarakë, kuzhinierë, shoferë kamionësh dhe përkthyes, mekanikë dhe teknikët e armëve.[13] Shërbimet PMC/PSC ndahen në gjashtë fushat e mëposhtme:

a. Lufta - Mund të përfshijë një spektër aktivitetesh, nga angazhimi i drejtpërdrejtë deri tek ofrimi i ndihmës për trupat e rregullta.

b. Stërvitje - Përfshirë jo vetëm armët dhe stërvitjen luftarake, por trajnimin në fusha të tilla si taktikat, ngasja jashtë rrugës dhe mjekësia në terren.

c. Mbështetje- Duke mbuluar fusha të tilla si logjistika, ndërtimi, mirëmbajtja dhe shërbimet e IT.

d. Siguria - Më e dukshme, mbrojtja e individëve, ndërtesave dhe infrastrukturës tjetër, si dhe transportuesit.

e. Inteligjenca - Mbledhja dhe analiza e informacionit, përmes metodave të tilla si kërkimi dhe mbikëqyrja.

f. Rindërtimi - në situata pas konfliktit, aktivitete të tilla si pastrimi i minave, rindërtimi i infrastrukturës dhe restaurimi i shërbimeve kritike.[14]

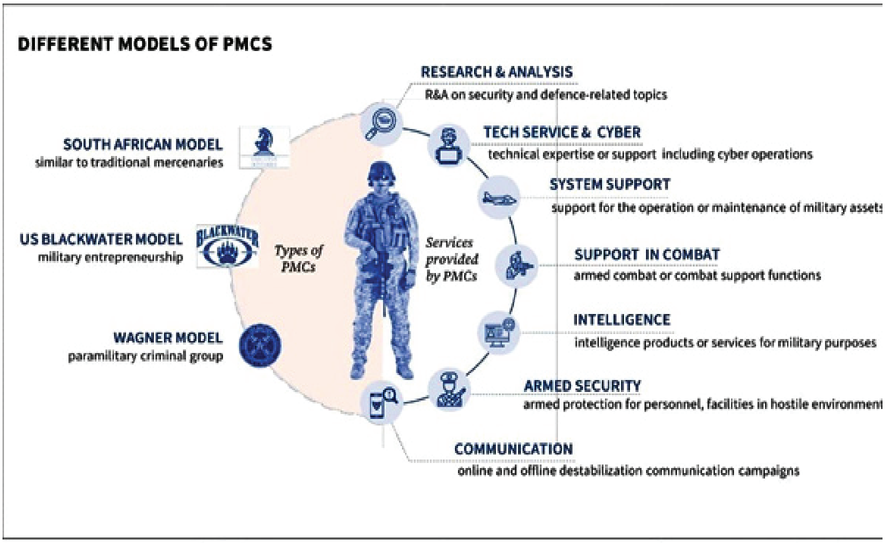
Në varësi të vendeve ku veprojnë, PMC/PSC-të kryejnë një gamë të gjerë detyrash luftarake ose ushtarake. Këto kompani madje operojnë nën shumë modele të ndryshme të PMC/PSC. Disa janë të integruar plotësisht në aparatin ushtarak shtetëror, ndërsa të tjerët veprojnë në një mënyrë më të ngjashme me rolin tradicional të mercenarëve[15].

---

[13] Isenberg, D. (2009). *Private Military Contractors and U.S. Grand Strategy.* Greenwood: International Peace Research Institute.

[14] Peter Hough,Andrew Moran, Bruce Pilbeam and Wendy Stokes. (2020). *International Security Studies, Theory and Practice* . London: Routledge.

[15] Union, C.o. (August). The Business of War – Growing risks from Private Military Companies. *Art - Research Paper*, 3.


DIFFERENT MODELS OF PMCS
SOUTH AFRICAN MODEL
similar to traditional mercenaries
US BLACKWATER MODEL
military entrepreneurship
BLACKWATER
WAGNER MODEL
paramilitary criminal group
Types of PMCs
Services provided by PMCs
RESEARCH & ANALYSIS
R&A on security and defence-related topics
TECH SERVICE & CYBER
technical expertise or support including cyber operations
SYSTEM SUPPORT
support for the operation or maintenance of military assets
SUPPORT IN COMBAT
armed combat or combat support functions
INTELLIGENCE
intelligence products or services for military purposes
ARMED SECURITY
armed protection for personnel, facilities in hostile environment
COMMUNICATION
online and offline destabilization communication campaigns

Problemi kryesor mund të jetë ndryshimi midis Kontraktorëve Ushtarakë Privatë/ Kontraktorëve Privatë Sigurisë modernë dhe atyre kontraktorëve tradicionalë të mbrojtjes, sepse nuk mund të thuhet se dallimi i një PMC/PSC nga një tjetër bazohet në funksionin e tyre kryesor, pasi është pothuajse e pamundur të ndahet. Një kontraktor nëse është modern ose tradicional, mund të sigurojë dhe të kryejë më shumë se një aftësi në çdo kohë të caktuar, në varësi të kërkesës operacionale.

Këtu vlen të përmendet dokumenti "Montreux", i përbërë nga dy pjesë, sipas të cilit PMC-të janë subjekte biznesi private që ofrojnë shërbime ushtarake dhe/ ose sigurie, pavarësisht se si e përshkruajnë veten. Shërbimet ushtarake dhe të sigurisë përfshijnë, në veçanti, mbrojtjen e armatosur dhe mbrojtjen e personave dhe objekteve, si autokolona, ndërtesa dhe vende të tjera; mirëmbajtjen dhe funksionimin e sistemeve të armëve; paraburgimi i të burgosurve dhe këshilla ose trajnime të forcave lokale dhe personelit të sigurisë[16].

Paralelisht me zhvillimin e tyre, kompanitë private ushtarake dhe të sigurisë edhe në të ardhmen do të paraqesin sfidë të vërtetë për rregullimin efektiv të drejtë të shërbimeve të tyre, sidomos në fushën e përgjegjësisë së tyre për shkeljen e të drejtave të njeriut gjatë përdorimit operativ. Por, sido që të jetë, ato do të vazhdojnë të ofrojnë shërbime malinje për agjencitë inteligjente, sigurisht duke i ikur radarit të atij shteti ku operon kjo kompani, qoftë ushtarake apo private e sigurisë.

---

[16] International Committee of the Red Cross, Government of Switzerland. (2020, June 11). *International committee of the red cross.* Retrieved from icrc: https://www.icrc.org/en/publication/0996-montreux-document-private-military-and-security-companies

Përfundime

Pohimet se PMC/PSC janë më ekonomikisht të arsyeshme se sa të mbahen ushtri të përhershme zakonisht bazohen në bazë të argumenteve të mëposhtme:

- PMC/PSC mund të punësojë personel që shpesh herë është i paguar në mënyrë të konsiderueshme më pak.
- Qeveritë ose organizatat që i huazojnë, nuk është patjetër t'iu sigurojnë PMC/PSC-ve përfitime të "fshehura" të tilla si: pensionet, mbrojtjen shëndetësore, vendbanim etj., sepse kjo është zakonisht e përfshirë në marrëveshje.
- PMC/PSC kanë aftësi menjëherë të rrisin numrin e forcave, pa harxhime për shkak të mirëmbajtjes afatgjatë të kapaciteteve ushtarake/sigurisë.
- Me atë që do t'i kryejnë operacionet kryesore jo luftuese apo luftuese, PMC/PSC u mundësojnë forcave të armatosura të përqendrohen në misionet thelbësore.
- Duke pasur parasysh se paguhen në bazë të marrëveshjes, në vend si funksion të numrit të ushtarëve në teren, është e vështirë të krahasohet arsyeja ekonomike e PMC/PSC kundrejt të ushtrisë së rregullt.
- Personeli i PMC/PSC shpesh merr trajnim që e siguron shtetin në cilësinë e anëtarëve të ushtrive kombëtare, ky trajnim në mënyrë efektive paraqet ndihmë financiare për vetë kompanitë në dhe operacioneve të tyre, kur personeli do të shkojë në vende pune të paguara më mirë në sektorin privat.
- Shërbimet inteligjente do të vazhdojnë të shfrytëzojnë këto struktura për të ikur mbikëqyrjes nga sistemi legjislativ dhe atij penal në vendet e tyre por edhe nga vendet ku do të përdoren këto struktura.

Rekomandime

1. Të krijohet autoriteti rajonal, ballkanik dhe ndërkombëtar që përcakton rregullat dhe normat e përgjithshme për KPM si dhe kontrollin e kontraktorëve ushtarakë privatë të regjistruar në këtë mekanizëm kontrolli.

2. Për vendet e Ballkanit duhet të ketë një specifikim brenda ligjeve të tyre kombëtare që hapja e kompanive që ofrojnë module leksionesh me elementë ushtarakë dhe policorë, duhet të vendosë kritere dhe specifika ku kontrolli i tyre duhet të bëhet nga ekspertët ushtarakë të vendit që zhvillon aktivitetin.

3. Personat që hapin kompani private ushtarake/sigurisë në vendet e rajonit të Ballkanit nuk duhet të lejohen të jenë persona që nuk janë shtetas të atij vendi, kështu që do të jete e pamundur që boshllëqet ligjore të përdoren nga persona

të lidhur me FSB-në ose Rusinë. GRU dhe vende të tilla si Serbia, Bosnja, Kroacia, Mali i Zi, Maqedonia e Veriut, Shqipëri dhe Kosova nuk duhet të jenë ofrues dhe prodhues të mercenarëve modernë (PMC/PSC) në mënyrë që njerëzit me tendenca terroriste të fshihen pas tyre.

- Dhe së fundi, bota perëndimore duhet të kuptojë se PMC-të do të përcaktojnë "luftërat e ardhshme" dhe fushat e betejës së shekullit të 21-të.

Bibliografia

1. https://balkaninsight.com/2024/05/09/win-win-game-western-balkans-should-up-arms-flows-to-ukraine/
2. https://library.fes.de/pdf-files/bueros/kosovo/20922-20240122.pdf
3. https://carnegieendowment.org/russia-eurasia/politika/2023/04/whats-behind-the-posturing-of-russian-mercenaries-in-the-balkans?lang=en
4. https://molfar.com/en/blog/catalog-of-russian-pmcs
5. https://jamestown.org/program/russian-pmcs-war-veterans-running-patriotic-youth-camps-in-the-balkans-part-one/
6. Javaid, A. (2021, Jul 6). *jagranjosh*. Retrieved from jagranjosh: https://www.jagranjosh.com/general-knowledge/private-military-company-pmc-and-its-working-1625585527-1
7. Armin, K. (2007, August 10). *researchgate.* Retrieved from researchgate:https://www.researchgate.net/publication/349325583_PRIVATNA_SIGURNOST
8. Isenberg, D. (2009). *Private Military Contractors and U.S. Grand Strategy.* Greenwood: International Peace Research Institute
9. Peter Hough,Andrew Moran, Bruce Pilbeam and Wendy Stokes. (2020). *International Security Studies, Theory and Practice* . London: Routledge.
10. Union, C. o. (August). The Business of War – Growing risks from Private Military Companies. *ART - RESEARCH PAPER*, 3.
11. International Committee of the Red Cross, Government of Switzerland. (2020, June 11). *INTERNATIONAL COMMITTEE OF THE RED CROSS.* Retrieved from icrc: https://www.icrc.org/en/publication/0996-montreux-document-private-military-and-security-companies

NATO në Ballkanin Perëndimor: Shqipëria nga "armiq", te motoja "miq besnik"

Prof. Asoc. Dr. Etleva SMAÇI
Zëvendësrektor i Akademisë së Forcave të Armatosura

Trajtesë e shkurtuar.

Ky punim synon të analizojë metamorfozën e qëndrimit dhe të rolit të NATO-s në Ballkanin Perëndimor[1] *në tre dekadat e fundit në raport me qëndrimin dhe rolin gjatë Luftës së Ftohtë.*

Për të realizuar këtë analizë krahasuese punimi do t'i referohet kontekstit historik ushtarak gjatë Luftës së Ftohtë, në mënyrë të veçantë faktit se shumica e shteteve të Ballkanit Perëndimor që sot aderojnë në NATO, ishin pjesë e Jugosllavisë, një vend që ndoqi politikën "jashtë aleancave dhe blloqeve ushtarake". Argumenti bazik që punimi do të sjellë është se shpërbërja e ish-Jugosllavisë në vitet 90-të si dhe ndryshimi i formës së regjimit në shtetet të caktuara, nxiti aleancën të ndryshonte qëndrim dhe të përfshihej në një zonë që e kishte konsideruar për 40 vjet "out of area", në mënyrë specifike për faktin se të drejtat e njeriut ishin të dhunuar në mënyrë masive.

Teza tjetër e punimit do të hedhë dritë mbi implikimet në rajon si pasojë e përplasjes së interesave NATO-Rusi, pas ndryshimit të balancave gjeostrategjike në favor të aleancës. Kjo tezë natyrshëm ngre dilemën nëse përfshirja e NATO-s në rajon do t'i shërbejë stabilitetit, apo do të jetë terren i

---

[1] Në këtë punim termi "Ballkan Perëndimor" do t'i referohet 6 shteteve: Shqipëri, Serbi, Mali i Zi, Maqedoni e Veriut, Bosnje–Hercegovinë dhe Kosovë.

përshtatshëm përplasjesh pikërisht për shkak të së shkuarës historike, ku vetë aleanca ka pas ndjekur teorinë e "hot patatoe".

Së fundmi, po jo më pak e rëndësishme, teza e tretë e punimit do të lidhet me anëtarësimin e Shqipërisë në NATO si një ish-vend i Traktatit të Varshavës dhe më një trashëgimi komuniste. Analiza historike e rastit të Shqipërisë do të bëhet e lidhur ngushtë me vendet e tjera anëtare të rajonit, për të shpjeguar nëse kemi një mbyllje të ciklit të Luftës së Ftohtë në Ballkanin Perëndimor, apo një variant modern të saj.

Fjalë kyçe: Ballkan Perëndimor, NATO, rreziqe, siguri, Luftë e Ftohtë.

Hyrje

Organizata e Atlantikut Verior u themelua më 1949 me qëllimin e qartë të mbrojtjes së Europës Perëndimore nga agresionet e mundshme të Bashkimit Sovjetik dhe aleatët e saj. Edhe pse për gjatë viteve të Luftës së Ftohtë u krijua ideja se NATO ishte jashtë Ballkanit (duke ruajtur zonat e influencës të vendosura në Jaltë), në fakt përfshirja e Greqisë dhe Turqisë në NATO dhe krijimi i Paktit Ballkanik me prezencën e Jugosllavisë më 1953, japin më tepër idenë e një pranie të kujdesshme në rajonin tonë. Me rënien e regjimit komunist në vendet e bllokut socialist në vitet 1990-1991 "hija kërcënuese" e agresionit sovjetik erdhi e u zhbë shumë shpejt. Për këtë ndihmoi në mënyrë të veçantë shpërbërja e kundërpartit të NATO-s, Traktatit të Varshavës. Në vazhdim të idesë së mësipërme, prania e "NATO"-s jo në pak qarqe u konsiderua e "tepërt", pasi ajo e kishte përmbushur misionin e saj historik, ruajtjen e perëndimit nga ideologjia komuniste. Aq më pak, ajo që nuk u parashikua në momentin e parë të rënies së komunizmit, ishte ambicia e NATO-s për të plotësuar vakumin e lënë në të gjithë Evropën Qendrore dhe Lindore.

Por pikërisht ndryshimet e regjimit do t'i ballafaqonin vendet komuniste me sfida të reja sigurie të cilat nuk mund të menaxhoheshin më me modelin e shtetit të "diktaturës së proletariatit". Ndërsa është fare i justifikueshëm vetë ofrimi i pjesës dërrmuese të vendeve të Evropës Lindore dhe Qendrore për t'u bërë pjesë e një organizate sigurie kolektive si NATO[2], të panjohurat që kanë kërkuar gjithmonë një përgjigje lidhen me "rinovimin" e NATO-s në një zonë të cilët e kishte konsideruar “out of area”. E mbi të gjitha “afrimi” pikërisht kur “kërcënimi” i komunizmit nuk ishte më prezent dhe alibia e Luftës së Ftohtë kishte rënë.

---

[2] Strobe Talbott: *The Russia Hand*, The Random House Trade Paperback Edition, 2003, p:94, Shtysa fillestare për zgjerim erdhi nga presidentët e tre ish-vendeve të Paktit të Varshavës. Në prill 1993, Lech Walesa i Polonisë, Vaclav Havel i Republikës Çeke dhe Arpad Goncz i Hungarisë iu lutën Bill Klintonit për pranimin e vendeve të tyre si anëtarë të NATO-s. Estonia bëri një kërkesë të ngjashme në maj, duke argumentuar se kjo ishte thelbësore për të parandaluar një ri-okupim të ardhshëm rus.

Nga pikëpamja historike, duke iu referuar dokumenteve të adoptuara nga kryetarët e shteteve anëtare të NATO-s më 1991, në atë çka u konsiderua koncepti i ri strategjik i Aleancës, mund të pohojmë se “zgjerimi i gardhit” u pa si e vetmja rrugë për të ruajtur “balancën strategjike në Evropë”.[3] Nga ana tjetër, nëse i referohemi preambulës së Traktatit të Uashingtonit, shtetet e anëtarësuara në NATO nuk e bazojnë unitetin e tyre thjesht në kundërshtimin e komunizmit, por më së pari në vlerat e përbashkëta siç janë: mbrojtja e lirisë, parimet demokratike, shteti ligjor etj. Për rrjedhojë ky argument i fundit ishte elementi kyç që frymëzoi strategjinë e zgjerimit në vendet e dala nga komunizmi.[4] Si rezultat që prej Samitit të Rigës më 2006, të gjitha vendet e Ballkanit Perëndimor kishin institucionalizuar marrëdhëniet me NATO-n nëpërmjet PfP ose nëpërmjet Këshillit të Bashkëpunimit Euroatlantik.

Por 75-vjetori i NATO-s dhe deklasifikimi i një sërë dokumentesh të panjohura për publikun gjatë këtij viti riktheu edhe një herë vëmendjen e studiuesve te pyetja: nëse ky zgjerim ku përfshiheshin një pjesë e mirë e ish-vendeve anëtare të Traktatit të Varshavës si dhe ish-republikave sovjetike ishte i drejtë apo shërbeu dy dekada më vonë si frymëzim për liderin nacionalist të Moskës, Vladimir Putin për një revansh ushtarak si ai ndaj Ukrainës?

Nëse marrim në shqyrtim tezën se zgjerimi në fund të viteve 90-të dhe në fillim të shekullit të 21-të i ka shërbyer “inkurajimit” të armiqësisë me Rusinë, duhet të shohim në retrospektivë disa nga parashikimet e bëra nga figura shumë të rëndësishme të marrëdhënieve ndërkombëtare. Le ta nisim me Henry Kissinger, i cili në janar të 1997 paralajmëronte se “herët në shekullin e ri, pas shumë ngritjeve dhe uljeve Rusia ka të ngjarë të ketë rivendosur autoritetin e saj qendror. Kjo mund të jetë shumë më pranë strukturave të favorizuara nga Pinoçeti ose Salazari se sistemet pluraliste perëndimore megjithëse ai do të jetë më i lirë se komunizmi”.[5]

E ardhmja e paparashikueshme e Rusisë që u vërtetua se nuk ishte një konstatim i gabuar nga ana e Kissinger, bëri që po në të njëjtën periudhë Zbignie Brzezinksi dhe Anthony Lake e shihnin zgjerimin si të vetmen mënyrë për të mbajtur lidhjen e Atlantikut të fortë. Zgjerimi i aleancës parashikonin Brzezinksi dhe Lake siguronte një mbrojtje kundër mundësisë së pamundur por shumë reale që Rusia t'i rikthehet sjelljes së kaluar."[6] Ky do të ishte një moment shumë i rëndësishëm për vendet e Europës Lindore dhe Ballkanit Perëndimor për t'u kthyer në rajone të rëndësishme për Aleancën e Atlantikut, kurse për këtë të fundit do të shënohej një kthesë e jashtëzakonshme pasi do të ofronte mbrojtje kolektive dhe siguri për ato vende të cilat deri në pak kohë më parë ishin konsideruar "armiq".

---

[3] North Atlantic Treaty Organization, “The Alliance’s Strategic Concept,” Agreed by the Heads of State and Government Participating in the meeting of the North Atlantic Council in Rome on 7-8 November 1991, paragrafi. 21.

[4] “The North Atlantic Treaty Preamble,” North Atlantic Treaty Organization, March 5, 2018, http://www.nato.int/cps/en/natohq/official_texts_17120.htm.

[5] Henry Kissinger, A World We Have Not Known, *Newsweek*, 27 January 1997

1. NATO dhe ish-Jugosllavia

Rajoni i Ballkanit i viteve 90-të jo në pak raste konsiderohej për NATO-n "një dhimbje koke".[7] Bazuar në studimet rreth marrëdhënies së NATO-s me vendet ish-komuniste të rajonit, rasti i Jugosllavisë ka qenë një test shumë i rëndësishëm në sfidën e zgjerimit. Këtu do të shmangim analizën e ndërhyrjeve humanitare të kryera nga NATO që prej përfshirjes së saj me një personel prej gati 100 vetash në Bosnje-Hercegovinë më 1992 e deri tek rasti i Kosovës. Fokusi i këtij sythi është analiza e faktorëve politikë dhe ushtarakë që kushtëzuan përfshirjen në NATO të ish-republikave të dala nga shpërbërja e Jugosllavisë. Pyetja direkte është se përse shtetet e pavarura të krijuar pas shpërbërjes së Jugosllavisë si Mali i Zi dhe Republika e Maqedonisë së Veriut nuk ruajtën trashëgiminë titiste të qëndrimit "jashtë blloqeve"? Trashëgimi që vazhdon të "trumbetohet" nga Serbia, pasardhësja legjitime e ish-Jugosllavisë e cila zyrtarisht ka statusin e një shteti neutral dhe që respektohet plotësisht nga aleanca[8].

Epoka e re e real-politike dhe lufta gjeopolitike që ndoqi përfundimin e Luftës së Ftohtë nuk vë dyshime mbi tezën se Shtetet e Bashkuara të Amerikës kishin dhe kanë një plan tepër ambicioz për Ballkanin Perëndimor dhe demokracitë e reja në këtë rajon. Hapi i parë i ambicies nuk mund të ishte veçse përfshirja e tyre në një sistem kolektiv sigurie (NATO), të cilën ato e kishin krijuar së bashku me aleatët e tyre menjëherë pas përfundimit të Luftës së Dytë Botërore. Qëllimin e kësaj përfshirje e sqaron mjaft qartë zoti Richard Holbrooke duke e lidhur me rolin udhëheqës në Evropë të Shteteve të Bashkuara të Amerikës me “krijimin e një sistemi sigurie që do të stabilizonte gjithë Evropën Perëndimore si dhe satelitët e Bashkimit Sovjetik në Evropën Qendrore.” [9] Për zotin Hoolbroke zgjerimi i NATO-s nuk ishte gjë tjetër veçse një pasojë e ngritjes së Perdes së Hekurt për 45 vjet.[10]

---

[6] Zbigniew Brzezinski and Anthony Lake, "The Moral and Strategic Imperatives of NATO Enlargement". *International Herald Tribune*, 1 July 1997.

[7] Elena Zamfiresku, NATO and Balkans, *Perceptions Journal of International Affairs,* March-May 1999, Volume IV, Number 1.

[8] Pas politikave neutrale të Serbisë, e cila tashmë është e rrethuar nga shtete anëtare të NATO-s, padyshim ka arsye të mjaftueshme dhe të dukshme. Së pari, një nga arsyet e qëndrimit të Serbisë larg NATO-s lidhet me lidhjet e ngushta me Rusinë, lidhje tradicionale dhe së dyti, opinion publik është një ndër kundërshtarët më të fortë, nisur nga bombardimet e vitit 1999, gjatë luftës së Kosovës.

Po cila ishte dhe mbetet pika më e dobët e vendeve të Ballkanit? Shteti socialist ia la vendin një shteti kapitalist, bazuar në ekonominë e tregut dhe demokracinë parlamentare. Kjo mund të konsiderohej si një “rend i ri “ për Ballkanin. Ose e thënë ndryshe një përpjekje për të rritur demokracinë në një terren tepër vulnerabilë. Pra, “detyrat” e NATO-s nuk u kufizuan thjesht në atë çka në periudhën e Luftës së Ftohtë ishte konsideruar një ombrellë mbrojtëse ushtarake kundër një agresioni. Përkundrazi, paqëndrueshmëria dhe pasiguria politike e prodhuar nga demokracitë “new born” në Ballkan që vazhdojnë të klasifikohen regjime hibride kanë ndikim në zonën e sigurisë së NATO-s. Për rrjedhojë, zgjerimi ishte i detyrueshëm duke i shërbyer interesave të stabilitetit të anëtarëve më të hershëm të organizatës.

Marrëdhënia e pas vitit 1990 ndërmjet NATO-s dhe Ballkanit është një nga ilustrimet më bindëse të kapacitetit të qenësishëm të NATO-s për t’u përshtatur me sfidat e reja. Edhe pse e padëshiruar nga askush, historia tragjike e shpërbërjes së ish-Jugosllavisë dhe pasojat e saj pasuese kanë luajtur, në një farë mënyre, rolin e një katalizatori për përshtatjen e Aleancave ndaj sfidave dhe rreziqeve të reja të periudhës së pas Luftës së Ftohtë. Nga ana tjetër, përshtatja e NATO-s ka favorizuar si vullnetin ashtu edhe aftësinë e saj për t’u bërë një instrument thelbësor për rilidhjen graduale të të gjithë zonës me rrjedhën kryesore të Evropës. Ky zgjerim jo vetëm u konsiderua i “shëndetshëm”, por pati edhe perifrazime se nëse NATO nuk do të dilte jashtë zonës së Luftës së Ftohtë, do të dilte jashtë biznesit”.[11] Në fakt, megjithatë, nuk ishte shqetësimi për të dalë jashtë biznesit për të nxitur operacionet e para të zbatimit të paqes në Ballkanin Perëndimor. Përkundrazi, vendet që iu bashkuan aleancës nxorën mësime nga e shkuara e tyre historike se një NATO në rritje ishte e vetmja organizatë ndërkombëtare që, me strukturën e saj të integruar të komandës ushtarake dhe përvojën e stërvitjeve të përbashkëta aleate, ishte organizata e duhur që të kryente operacionet e menaxhimit të krizave dhe paqeruajtëse përtej kufijve të saj, çka nënkuptonte një terren krizash si Ballkani Perëndimor, për t’u përdorur nga aktorë të tjerë. Vlen të mos anashkalohet fakti që si Mali i Zi, ashtu edhe Maqedonia e Veriut e kanë parë anëtarësimin në NATO si një kriter përmbushës për integrimin e tyre në Bashkimin Evropian, edhe pse deri më tash nuk ka dhënë rezultatet e pritshme.

---

[9] Richard Holbrooke, *“America, A European Power”,* Foreign Affairs, March/April l995, page 39.

[10] Po aty…faqe 43.

[11] Senator Richard Lugar. NATO*: Out of Area or Out of Business. A Call for U.S. Leadership to Revive and Redefine the Alliance* (Washington, DC: Overseas Writers Club, 24 June 1993).

2. Shqipëria nga Varshava në NATO

Në historikun e zgjerimit të NATO-s në Ballkanin Perëndimor, Shqipëria vlen të trajtohet si një rast studimor jo vetëm se në fund të viteve 60-të do të guxonte të dilte nga rivali i NATO-s, Traktati i Varshavës, por edhe për faktin tjetër se ishte ndër të parat vende ish komuniste që me rënien e regjimit, tregoi një angazhim të lartë për t'u bërë pjesë e NATO-s. Përgjatë Luftës së Ftohtë mjedisi gjeostrategjik në rajon përbënte një pazëll shumë interesant. Dy nga fqinjët tanë me të cilët ndanim kufirin detar Italia dhe Greqia ishin anëtarë të NATO-s. Bregdeti italian shërbente si terren dislokimi për Flotën VI amerikane. Përsa i përket Greqisë edhe aty kishte disa baza të NATO-s me qëllim parësor ruajtjen e Mesdheut nga kërcënimi i Bashkimit Sovjetik.

Pikërisht zgjidhja "ex deux machine" e këtij rebusi do të bëhej Shqipëria komuniste që do t'i jepte një mundësi të artë Moskës për balancimin e forcës në Mesdhe me pozitën e saj gjeografike. Anëtarësimi i Shqipërisë në Traktatin e Varshavës në historinë politike dhe ushtarake të Luftës së Ftohtë është tashmë i dëshmuar si një lëvizje pragmatiste e qeverisë komuniste për të siguruar integritetin territorial të vendit nën "ombrellën" e një organizmi politik dhe ushtarak të sigurisë kolektive të bllokut komunist që drejtohej nga Bashkimi Sovjetik.[12] Me praninë e trupave ushtarake të Bashkimit Sovjetik në bazën detare të Pashalimanit dhe ajo e Sazanit do të zinte fill e do të rritej ndjeshëm rivaliteti me NATO-n.

NATO trajtohej si "armik" dhe rrezik për shtetin shqiptar jo vetëm në literaturën politike, por edhe në manualet dhe doktrinat ushtarake. Por njohja e ushtrive të saj ishte një pjesë shumë e rëndësishme e edukimit ushtarak të asaj periudhe. Vlen të theksohet se qëndrimi i NATO-s ndaj Shqipërisë komuniste ishte mjaft i ndjeshëm në vitet 1955-1961, kur Bashkimi Sovjetik vendosi një bazë nëndetëse në gjirin e Vlorës. Përsa i përket qëndrimit që NATO mbajti pas përjashtimit *de facto* të Shqipërisë nga Traktati i Varshavës, ishte adoptimi i politikës "hands off" (mosndërhyrjes) propozuar nga George Kennan në raportin e tij të shkurtit të vitit 1962.[13] Largimi i trupave sovjetike lehtësoi pozitat e NATO-s në Mesdhe, por afrimi me Shqipërinë, një vend komunist u kalkulua nga NATO si një mundësi konflikti me Traktatin e Varshavës. Kjo politikë mori fund me shpërbërjen e Traktatit të Varshavës dhe rënien e komunizmit. E dalë nga një izolim diktatorial, Shqipëria shprehu interes për dialog me NATO-n duke u bërë anëtare e Këshillit të Bashkëpunimit të Atlantikut të Veriut (NACC) në qershor 1992. Rrugëtimi drejt NATO-s zgjati gati dy dekada.[14] Vlen të theksohet se procesi i anëtarësimit pati karakteristika të ngjashme me atë të Traktatit të Varshavës në dy element: propagandimi politik me natyrë partiake si dhe entuziazmi popullor rreth anëtarësimit. Ky i fundit shpesh u keqinterpretua dhe u trajtua si një afrim me SHBA sesa me një organizatë të sigurisë kolektive.[15] Kjo shpjegon edhe të dhënat statistikore që dëshmojnë se rreth 90% e popullatës ishte pro anëtarësimit në NATO (shumë të ndryshme me vendet e tjera ballkanike).

---

[12] Etleva Smaçi, *Shqipëria në Traktatin e Varshavës,* UETPRESS, Tiranë:2023.
Shqipëria hyri në Traktatin e Varshavës në vitin 1955, duke suprizuar më së shumti Lindjen sesa Perëndimin. Reagimi lidhej me shumë faktorë, duke nisur nga varfëria e tejskajshme e vendit komunist si dhe nga ndryshimi i politikës së Kremlinit. Politika e ndjekur nga Hrushovi pas vdekjes së Stalinit çoi në zgjerimin e hartës së vendeve komuniste të përfshira në një aleancë ushtarake në një rajon tepër të brishtë, siç ishte Ballkani.

[13] National Archives Record Administration (NARA), Records of the U.S Departament of State Relating to International Affairs of Albania, 1960-1963, Box 1926, November 17, 1961.

Partneriteti për Paqe ishte një mekanizëm shumë i rëndësishëm për përgatitjen e ish-vendit komunist dhe anëtar i Traktatit të Varshavës për anëtarësimin përfundimtar në NATO[16]. Anëtarësimi i Shqipërisë në NATO erdhi si rrjedhojë e vendimit të rëndësishëm për zgjerimin e Aleancës, të marrë më 3 prill 2008 nga të 26 krerët e shteteve dhe qeverive të Aleancës gjatë një seance të posaçme të Samitit të NATO-s Bukuresht, nëpërmjet të cilit Shqipëria dhe Kroacia u ftuan të fillonin bisedimet për anëtarësimin. Paraqitja e parë e Shqipërisë si anëtare me të drejta të plota e NATO-s u bë në Samitin e Aleancës që u mbajt në Strasburg/Kehl më 4 prill 2009, ndërkohë që më 7 prill 2009, në selinë e Aleancës në Bruksel, u zhvillua ceremonia zyrtare e ngritjes së flamujve të Shqipërisë në NATO.

Që prej fillesave të këtij rrugëtimi anëtarësimi i Shqipërisë në NATO është parë i lidhur ngushtë jo vetëm me reformat në sektorin ushtarak, por në radhë të parë me demokratizimin e jetës në vend, me luftën kundër korrupsionit dhe krimit të organizuar. Në dallim të plotë nga qasja tradicionale ideologjike e regjimit komunist, ajo që duhet ta bënte të denjë Shqipërinë për NATO-n ishte jo vetëm pranimi por edhe përshtatja e me vlera e përbashkëta që simbolizonin aleancë: sistemi pluralist, demokracia, liria dhe toleranca.[17] Shqipëria në dallim nga vendet e tjera të rajonit nuk ka pasur problem faktorin rus në lidhje me anëtarësim e saj në NATO, por kjo nuk do të thotë që anëtarësimi është parë me sy pozitiv nga Moska. Veçanërisht angazhimet e fundit të qeverisë shqiptare për rijetësimin e disa bazave ushtarake (si rasti i Kuçovë) me një të shkuar historike të afërt me Traktatin e Varshavës, bënë që shtypi t'i rikthehej trashëgimisë së kampit sovjetik.[18] Edhe përpara hapjes së bazës së Kuçovës, Sputnik Serbia dhe platformat e tjera ruse që veprojnë më Ballkan nuk kanë nguruar të furnizojnë me lajme të rreme, duke portretizuar Shqipërinë se do të përdoret si një "korridor lufte" nga NATO.[19] Shqipëria konsiderohet "një shtet kukull" që po përdoret nga Aleanca për të rimilitazuar territore të cilat sipas Sputnik tashmë konsiderohen "të zotëruara" prej NATO-s. Edhe rijetësimi i bazës së Kuçovës jo vetëm për shtypin, por edhe për një kategori studiuesish pro rus është trajtuar si një argument se "Perëndimi ka gënjyer që prej ditës së pare për sa i përket zgjerimit të tij në lindje në përfundim të Luftës së Ftohtë".[20]

---

[14] Përfshirja e Shqipërisë në aleancë u mbështet në disa instrumente siç ishin PfP dhe MAP për të mbërritur tek anëtarësimi më 2009.

[15] Institute for Democracy and Mediation. Albanian perceptions on NATO integration. Tirana June 2007 http://idmalbania.org/publications/en/AlbPerceptionOnNATOintegrations.pdf.

[16] Shqipëria iu përgjigj pozitivisht ftesës për PfP më 1994. Më vonë si rezultat i hapave pozitivë vendi ynë u përfshi në Planin e Veprimit për Anëtarësim (MAP) në 1999.

[17] NATO (2006b): Jaap de Hoop Scheffer, Secretary General, NATO, Speech at the Albanian parliament, 6 July, on-line text.

Ofrimi i territorit shqiptar për baza të NATO-s duket se nuk do të ndalet me rastin e bazës së Kuçovës, pasi në deklarimet e kryeministrit Edi Rama, në qershor të këtij viti, u përmend fakti se Shqipëria është në bisedime me NATO-n për të ndërtuar një bazë detare në Porto Romano[21], një port në ndërtim e sipër në bregdetin e saj Adriatik. Kjo deklaratë vinte pas asaj të muajit maj në lidhje me ofrimin NATO-s bazën e saj detare Pashaliman rreth 200 km (124 milje) në jug të Tiranës, e cila është tjetër trashëgimi sovjetike për të cilën Shqipëria ka akoma të hapur debatin me Moskën për 4 nëndetëset e ngelura në bazë në vitin 1961. Në përmbyllje të kësaj analize mbi paradigmën e Shqipërisë "nga armiq në miq besnikë" në raport me NATO-n, duket se pas 15 vitesh anëtarësim, Shqipëria, përsa parashtruam më lart, nuk është më thjesht një 'konsumatore' e sigurisë, por edhe një ofruese e saj veçanërisht për rajonin e Ballkanit Perëndimor.

3. Zgjerimi, stabilitet apo destabilitet?

Zgjerimi i NATO-s në Ballkanin Perëndimor në fazat e hershme të tij kaloi përmes një hezitimi të dukshëm. Ngurrimi u bë shumë i qartë në fillesat e luftës në ish-Jugosllavi. Vetë perceptimet e Aleancës nuk ishin pozitive për disa prej vendeve.[22] Pyetja që gjendet më shpesh në punimet shkencore është pikërisht: A ndikoi zgjerimi i të NATO-s në stabilizimin demokratik të shteteve postkomuniste në rajon? Pyetja lidhet edhe me debatin e krijuar në raport me ithtarët e zgjerimit të NATO-s Warren Christopher, Anthony Lake, William Perry, Strobe Talbot, etj., të cilët e kanë përdorur shpesh argumentin e ndikimit pozitiv të zgjerimit në konsolidimin e regjimeve demokratike në periudhën postkomuniste. Parashihej se zgjerimi i NATO-s në Ballkan do të mund të lejonte aleancën që të mos binte më në rolin e "importueses" së sigurisë, por të mund ta "eksportonte" atë në rajon, duke siguruar stabilitet përmes demokracisë dhe prosperitetit. Padyshim për vendet Ballkanike që janë anëtarësuar në NATO kjo është përkthyer në hapa të vështirë politikë, por jo të pamundur. Për të ndryshuar institucionet e tyre të vjetra të gjitha vendet e Ballkanit Perëndimor që aspironin të bëheshin pjesë e NATO-s u bënë pjesë e programeve të reja, ku më i rëndësishmi ngelet PfP (1994), që synim kryesor kishte forcimin e bashkëpunimit dhe ndërtimin e marrëdhënieve reciproke mes vendeve partnere.

---

[18] Jo në pak raste platforma të ndryshme iu referuan bazës së Kuçovës si "një bazë e periudhës sovjetike" Albania, wary of Russia, reopens Soviet-era air base to NATO | Reuters

[19] https://euronews.al/en/wars-of-the-west-propaganda-nato-will-attack-russia-through-albania-and-kosovo/
https://sputnikglobe.com/20240305/perennial-puppet-state-albania-logic. Kukulla e përhershme Shteti Shqipëri zgjedhje 'logjike' për NATO-n e riorganizuar

[20] Po aty.

[21] https://shqiptarja.com/lajm/rama-gati-te-bashkefinancojme-bazen-e-re-detare-te-natos-ne-porto-romano-nato-te-garantoje-kufirin-mes-kosoves-e-serbise.

Duke iu rikthyer përsëri momentit të parë kur Aleanca vendosi të zgjerohej dhe t'i hidhte sytë në territore të konsideruar "mollë e ndaluar", në vitin 1990 aleatët e kishin shumë të qartë se "në Evropën e re të krijuar siguria e çdo shteti ishte e lidhur pazgjidhshmërisht me sigurinë e fqinjëve të saj".[23] Të njëjtin argument e gjejmë edhe në pohimin e Strobe Talbot se "e gjithë Evropa do të jetë më e sigurt dhe më e begatë nëse vendet ish-komuniste do të mund të ecnin e të zhvilloheshin përmes shoqërisë civile, ekonomisë së tregut dhe marrëdhënieve harmonike me fqinjët ."[24]

Argumenti i Talbotit lidhet ngushtë me idenë e shkrimit të tij se prania e NATO-s në vendet ish-komuniste dhe në disa raste partnere apo satelite të Bashkimit Sovjetik, nuk ishte thjesht një mekanizëm frenimi i Rusisë, apo shtrëngues, por një instrument sigurie kolektive, ku përfshihej edhe vetë Rusia. Kjo shpjegon edhe arsyen përse theksi i aleancë me mbarimin e Luftës së Ftohtë u zhvendos nga mbrojtja e territorit të vendeve anëtare në mbrojtjen e interesave të përbashkëta duke u bërë një domosdoshmëri strategjike.[25] Por idetë e mësipërme i përkasin dekadës së fundit të shekullit të kaluar, kur Rusia ishte ende nën shokun e shpërbërjes dhe konsiderohej e “dobët”. Pas vitit 2014 optika ruse në lidhje me zgjerimet e NATO-s ka qenë trajtimi i anëtarësimeve të reja si përpjekje të NATO-s për ta organizuar rendin botëror sipas kufijve të rinj.

---

[22] Watkins dhe Srdjan Gligorijeviç, NATO dhe Ballkani: Shembulli për një integrim më të gjerë, Çështje *të Sigurisë,* Instituti për Ndërmjetësim dhe Demokraci, nr.5, Tiranë:2007.

[23] "*London Declaration on a Transformed NATO in the 21st century 26 Final March 19, 2001 North Atlantic Alliance,"* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council. London July 5-6, 1990, paragraph 4.

[24] Strobe Talbott, "Russia Has Nothing to Fear," *New York Times*, February 18, 1997.

[25] Dr. William J. Perry and Warren Christopher. "NATO's True Mission." The New York Times, October 21, 1997

Pyetja e parë që të vjen në mend është: A i vuri në rrezik marrëdhëniet NATO - Rusi zgjerimi i organizatës së Atlantikut Verior në rajonin e Ballkanit, i njohur si rajon ku influenca ruse ka qenë konstante në marrëdhëniet ndërkombëtare të shekullit XX dhe XXI?[26] A ja ka arritur NATO të krijojë stabilitet në rajon, argument që përdori për zgjerim apo zgjerimi ishte thjesht një pretekst si pretendon Moska?

Le të hedhim një vështrim mbi vendet e anëtarësuar së paku në 10 vjetët e fundit ku bëjnë pjesë Mali i Zi dhe Maqedonia e Veriut. Kjo e fundit është anëtarja më e re aleancës nga Ballkani Perëndimor. Në rastin e Maqedonisë së Veriut, përpara se t`i bashkohej aleancës, NATO, kreu tre operacione ushtarake për mbështetjen e paqes, të cilat përveçse kontribuuan në zgjidhjen e konfliktit të brendshëm, ndihmuan edhe në krijimin e kushteve të nevojshme për konsolidimin e demokracisë në këtë vend. Në eksperiencën ballkanike, rasti i Maqedonisë së Veriut shihet edhe si një shembull suksesi lidhur me çështjet e sigurisë në bashkëpunimin NATO-BE.[27]

Ajo që bie në sy në rastin e Maqedonisë së Veriut se anëtarësimi nuk pati një mbështetje të gjerë popullore. Qarqet nacionaliste me ndikim rus ushtruan ndikim te pjesë të caktuara të saj që nuk pajtohen me rolin e NATO-s. Rusia u përpoq të përfitonte nga vështirësitë e tilla për të penguar integrimin e Maqedonisë në NATO. Kremlini dënoi ndryshimin e emrit si imponim nga Perëndimi dhe këmbënguli që ai të rinegociohej në Këshillin e Sigurimit të OKB-së, një forum në të cilin ajo ka të drejtën e vetos. Gjithsesi, Rusisë i mungon afiniteti historik me Maqedoninë e Veriut në të njëjtën mënyrë që e lidh atë me Serbinë. Kështu që me anëtarësimin Rusia tani ka ulur interesin për Maqedoninë e Veriut. Kjo është vënë në dukje me zbutjen deklaratave publike të Kremlinit për çështjet maqedonase dhe zhvendosjen e agresivitetit te NATO për tërheqjen e vendeve të Ballkanit në aleancë.

I njëjti fenomen u vu re edhe pas anëtarësimit të Malit të Zi, në 2017 ku u kalua nga këndvështrimi kombëtar i çështjes në atë ndërkombëtar. Sjellja ndaj rastit të Malit të Zi dhe Maqedonisë është interpretuar si një rikthim i Rusisë në Ballkan, ku ajo kërkon të marrë rolin që ka pasur Perandoria Ruse deri në shpërbërjen e saj. Në këtë këndvështrim mund të konsiderohet një faktor i rëndësishëm për Putinin loja ballkanike nisur nga sentimentet nacionaliste të cilat i përdorë përpara elektoratit të tij dhe që për rrjedhojë e bëjnë politiken e jashtme të Rusisë më të paparashikueshme sesa atë të periudhës së Bashkimit Sovjetik gjatë Luftës së Ftohtë.

---

[26] Dimitar Bechev, *Rival Power, Russia in Southeast Europe’.* Yale University Press. Autori analizon tezën e panortodoksisë dhe pansllavizmit.

[27] Nënshkrimi i marrëveshjes së Ohrit, për të parandaluar luftën në ish-republikën jugosllave të Maqedonisë.

Së fundmi, siç e përmendëm edhe më lart mospërfshirja në NATO e një aktori me shumë peshë në Ballkan si Serbia e bën të vështirë krijimin e stabilitetit dhe të pashmangshëm ndikimin rus. Serbia qëndron si një “gjemb” midis një NATO-je në zgjerim dhe Rusisë, partnere tradicionale e Serbisë. A mund të reagojë kjo e fundit në mënyrë të dëmshme për rajonin? Rusia e drejtuar nga zoti Putin, një ish-sovjetik që kalon nga karrigia e kryeministrit në atë të presidentit nuk e ka “kapërdirë” dot politikën e “open door policy” të NATO-s.

Por për njohësit e mirë të politikës së jashtme të Putinit më shumë se një ringjallje e Rusisë së Madhe, kjo është një mënyrë për ta detyruar perëndimin ta shohë Moskën si lojtar të barabartë në tavolinë.[28] E thënë ndryshe, Putini po tenton në Ballkan bipolaritetin e Luftë së Ftohtë, pas një supermacie gati prej një dekade (1990–2000) të unipolaritetit të vendosur nga NATO. Zgjerimi në tërësi (jo vetëm në Ballkan) është konsideruar nga Moska (rrethet nacionaliste) si një Jaltë e dytë, por pa Rusinë. Stabiliteti për shumë studiues është zëvendësuar me termin “stabilokraci”, pasi vendet e anëtarësuara në NATO kanë ngelur larg integrimit në BE. Por qoftë Aleanca, qoftë vendet e rajonit, pranojnë se Ballkani Perëndimor ka nevojë që NATO të vazhdojë të mbetet politikisht e përkushtuar ndaj rajonit.[29]

Përfundime

Ballkani Perëndimor përbën investimin politik dhe operacional më të vjetër dhe më jetëgjatë të Aleancës, dhe sigurisht më sfiduesi duke pasur parasysh kompleksitetin rajonal dhe fragmentimin e tij politik, etnik dhe fetar. Rajoni përfshin: vende anëtare të NATO-s, partnerë të NATO-s, një vend neutral (Serbinë) dhe së fundi është rajoni ku NATO është ende duke kryer operacionin e vetëm ushtarak përmes KFOR-it në Kosovë.

Është e pamohueshme se në tërësi zgjerimi i NATO-s, duke përfshirë këtu edhe zgjerimin në Ballkanin Perëndimor, ka prodhuar debat në raport me qëllimet e Rusisë. Nëse i referohemi Henry Kissinger ai që në fillesat e zgjerimit të aleancës në Evropën Qendrore dhe Lindore deklarohej i shqetësuar për “hatërmbetjet” e Rusisë, që do të materializoheshin në “minime” të NATO-s në territoret e reja.

---

[28] Dimitar Bechev*, “Understanding Russia’s influence in the western Balkans”*, Semptember, 2018. Vizita e kancelares Angela Merkel dhe e Sekretarit të Mbrojtjes James Mattis në Shkup para referendumit të 30 Shtatorit, ishte një tregues se Rusia ishte gatshme për të minuar votën popullore dhe për ta manipuluar atë.

[29] Speech by NATO Secretary General Jens Stoltenberg previewing the NATO Summit in Brussels at event organised by NATO, The German Council on Foreign Relations (DGAP) and The Brookings Institution

Në optikën e politikës së jashtme të Putinit kjo do të përkthehej me teorinë e “zero sulme”, që do të thotë se çdo fitore e Perëndimit është humbje e pastër e Moskës. Zgjerimi i aleancës është parë nga Moska si një manifestim i aspiratave të Uashingtonit për hegjemoni në Ballkan, por për ta përmbyllur ndër të gjithë argumentet e sjella stabiliteti rajonal, kundër hegjemonisë, është arsyetimi strategjik që shpjegon më së miri zgjerimin e NATO-s në rajon. Në politikën e NATO-s, sigurisht që mund të identifikojmë një përpjekje për të kontribuar në stabilizimin demokratik të vendeve të Ballkanit Perëndimor që tashmë i janë bashkuar aleancës. Nga njëra anë, siç tregohet në këtë studim, shtytja drejt zgjerimit të NATO-s në rajonin tonë mund të mos ketë pasur ndikim aq të rëndësishëm në demokratizim sa shpresonin ithtarët e saj, të cilët e nisën këtë proces në mesin e viteve ‘90. Por ana tjetër, zgjerimi ka pasur një efekt shumë pozitiv në sigurinë euroatlantike. E thënë ndryshe aty ku “fqinjët” e NATO-s janë stabël, NATO është e “qetë dhe sigurt”.

Kjo do të thotë se aleanca është përpjekur të konsolidojë vizionin e përcaktuar nga sekretarja e shtetit Albright në takimin e vitit 1997, kur deklaronte se qëllimi i hapave të mëtejshëm të zgjerimit ishte që “të bëhej për Evropën Lindore ajo çfarë NATO kishte bërë 50 vjet më parë për Evropën Perëndimore: integrimi i demokracive të reja, eliminimi i urrejtjeve të vjetra, mbështetje në rikuperimin ekonomik dhe frenimi i konflikteve.”[30] Ngjarjet e ndodhura në Ballkan në fillim të viteve 90-të ndikuan fuqishëm në evolucionin e NATO-s pas Luftës së Ftohtë dhe anasjelltas prania aktive NATO-s në rajon jo vetëm ka parandaluar shpërthimin e armiqësive dhe zjarreve nacionaliste por ka ndihmuar secilin prej shteteve të Ballkanit Perëndimor që individualisht të bëhen pjesë e zonës euroatlantike në mënyrë të suksesshme. Larg mundësive të shpërthimit të konflikteve të armatosura serioze, paqja e rajonit mbetet e brishtë. Prandaj dhe aleanca duhet t’i rivlerësojë strategjitë ndaj rajonit për t’ju përgjigjur sfidave aktuale. Parandalimi dhe mbrojtja do të mbeten gur themeli i NATO-s dhe falë zbatimit praktik të politikës së dyerve të hapura të NATO-s, shumica e vendeve të Ballkanit Perëndimor, tani aleatë, kontribuojnë në mënyrë aktive në të. Prandaj është e gjithë pranuese tashmë se asnjë vizion i ardhshëm i NATO-s nuk mund të dështojë të lërë jashtë Ballkanin Perëndimor si një të tërë dhe jo thjesht në skemën e sotme 3 brenda, 3 jashtë.

---

[30] Madeleine K. Albright, Prepared Statement before the North Atlantic Council, NATO Headquarters, Brussels, Belgium, February 18, 1997.

Shënim: *Të gjitha idetë e shprehura në këtë artikull i përkasin autores dhe jo institucionit ku ajo punon.*

Bibliografia

1. ALBRIGHT, Madeleine. Prepared Statement before the North Atlantic Council, NATO Headquarters, Brussels, Belgium, February 18, 1997
2. BECHEV, Dimitar *"Understanding Russia's influence in the western Balkans"*, Semptember, 2018
3. BECHEV, Dimitar *Rival Power, Russia in Southeast Europe'.* Yale University Press.
4. BRZEZINSKI, Z and LAKE, A, *The Moral and Strategic Imperatives of NATO Enlargement.* International Herald Tribune, 1 July 1997.
5. KISSINGER, Henry, A World We Have Not Known, Newsweek, 27 January 1997
6. SMAÇI, Etleva.*Shqipëria* në Traktatin e Varshavës, UETPRESS, Tiranë:2023
7. TALBOTT, Strobe *The Russia Hand*, The Random House Trade Paperback Edition, 2003.
8. ZAMFIRESKU, Elena. *NATO and Balkans*, Perceptions Journal of International Affairs, March-May 1999, Volume IV, Number 1.
9. HOLBROOKE, Richard *America, A European Power*, Foreign Affairs, March/April l995.
10. Perry, W and Warren Christopher. *NATO's True Mission*. The New York Times, October 21, 1997.
11. WATKINS dhe GLIGORIJEVIÇ, S. *NATO dhe Ballkani*: Shembulli për një integrim më të gjerë, Çështje të Sigurisë, Instituti për Ndërmjetësim dhe Demokraci, nr.5, Tiranë:2007

Burime arkivore

12. National Archives Record Administration (NARA), Records of the U.S Departament of State Relating to International Affairs of Albania, 1960 -1963, Box 1926, November 17, 1961.

Burime interneti

13. Albania, wary of Russia, reopens Soviet-era air base to NATO | Reuters
14. https://euronews.al/en/wars-of-the-west-propaganda-nato-will-attack-

russia-through-albania-and-kosovo/ https://sputnikglobe.com/20240305/perennial-puppet-state-albania-logic

15. https://shqiptarja.com/lajm/rama-gati-te-bashkefinancojme-bazen-e-re-detare-te-natos-ne-porto-romano-nato-te-garantoje-kufirin-mes-kosoves-e-serbise
16. https://idmalbania.org/publications/en/AlbPerceptionOnNATOintegrations.pdf

Lufta hibride, roli i teknologjisë dhe i inteligjencës artificiale

Nënkolonel (R) Msc. Kanan HIMAJ

Trajtesë e shkurtuar.

Lufta hibride është ndër konceptet më të debatuara në shkencën bashkëkohore, në mënyrë të veçantë në atë të sigurisë dhe mbrojtjes. Një pyetje kritike ende e pazgjidhur është nëse koncepti përshkruan një fenomen krejtësisht të ri empirik? Shumë studiues pohojnë se lufta hibride është e re vetëm për aq sa teknologjitë e reja përdoren si armë lufte. Prandaj, sot shumë studiues dalin në përfundimin se lufta hibride është e kufizuar në nivelet e sigurisë njerëzore, sepse risitë teknologjike nuk e ndryshojnë rrënjësisht mënyrën se si njerëzit marrin vendime strategjike.

Ky punim (leksion i orientuar) sfidon këtë supozim bazuar në marrëdhënien midis luftës hibride, teknologjisë bashkëkohore dhe inteligjencës artificiale[1]*. Natyrshëm shtrohet pyetja: Në çfarë shkalle ndikon shfaqja e inteligjencës artificiale në fenomenin e luftës hibride? Në këtë aspekt, shkrimi do të synojë të argumentojë që teknologjia mund të jetë e rëndësishme vetëm për nivelet më të ulëta të luftës, ndërsa inteligjenca artificiale ka implikime të nivelit strategjik për sjelljen dhe mbrojtjen kundër luftës hibride. Kështu, në epokën e luftës hibride, risia e inteligjencës artificiale nuk kufizohet në nivelet më të ulëta të luftës, por është e përhapur gjerësisht në thellësi dhe hapësirë.*

---

[1] Inteligjenca artificiale i referohet aftësisë së një kompjuteri për të kryer funksione dhe arsyetime që aktualisht janë tipike vetëm të mendjes njerëzore.

Duke pasur parasysh natyrën shkatërruese të teknologjive të bazuara në inteligjencë artificiale[2]*, komuniteti perëndimor i sigurisë duhet të thellojë studimet e orientuara nga inteligjenca artificiale përmes partneriteteve më të forta shkencore. Sfidat dhe mundësitë diskutohen shkurtimisht duke shqyrtuar një iniciativë të fundit të organizatës së Traktatit të Atlantikut të Veriut, të ashtuquajtur "Përshpejtuesi i Inovacionit të Mbrojtjes për Atlantikun e Veriut".*

Ky punim shqyrton konceptin e luftës hibride, duke ofruar një rishikim kritik të marrëdhënies së saj me teknologjinë; fazën aktuale të zhvillimit të inteligjencës artificiale në sfondin e hulumtimit të konfliktit; përshkruan se si inteligjenca artificiale mundëson dhe kundërshton luftën hibride edhe nëse kjo ka efekte strategjike dhe së fundmi, përshkruan implikimet për Perëndimin dhe përdor DIANA si një shembull të praktikave më të mira.

Fjalë kyçe: Luftë hibride, inteligjencë artificiale, inovacion mbrojtës, NATO, BE, institucionet arsimore dhe shkencore, teknologjia e informacionit.

Hyrje

Koncepti i luftës hibride mendohet si një qasje e re ndaj luftimeve që u shfaq pas Luftës së Ftohtë. Për Frank Hoffman, arkitektin kryesor të konceptit, janë metoda të ndryshme të kombinuara për të arritur sinergji në hapësirën e betejës.[3] Megjithatë, shumë studiues pohojnë se një luftë e tillë shumë modale ka ndodhur gjithashtu në të kaluarën e largët dhe janë skeptikë për luftën hibride që është një fenomen krejtësisht i ri.[4] Ata argumentojnë se lufta hibride është e re vetëm në atë shkallë që teknologjitë e reja, të tilla si aftësitë kibernetike, i shtohen përzierjes së metodave të luftimit.

Rrjedhimisht, risia e luftës hibride është e kufizuar në nivelin operacional dhe taktik të luftës. Sipas tyre, kjo ndodh se inovacioni teknologjik nuk ndryshon rrënjësisht mënyrën se si njerëzit marrin vendime në nivelin strategjik. Ky punim sfidon këtë supozim, duke analizuar marrëdhënien midis luftës hibride dhe inteligjencës artificiale. Inteligjenca artificiale shpesh është etiketuar si kufiri i ardhshëm teknologjik, por për dy koncepte gjerësisht të njohura, ka çuditërisht pak kërkime ndërdisiplinore mbi ndërveprimin midis luftës hibride dhe inteligjencës artificiale. Për aq sa ekzistojnë punimet aktuale, fokusohen në mënyrën se si aftësitë e inteligjencës artificiale mund të përdoren në skenarë specifikë të luftës hibride, si ndikimi ose operacionet kibernetike. Sulmet kibernetike në shkallë të gjerë ndaj infrastrukturave kritike dhe të rëndësishme të informacionit nga aktorë keqdashës kibernetikë të sponsorizuar nga aktorë shtetërorë, si ato të vitit të kaluar me origjinë nga Irani, dëshmojnë se siguria kibernetike duhet të marrë përparësi, në kuadër edhe të zhvillimit të digjitalizimit të shërbimeve publike për qytetarët[5].

---

[2] Teknologjia e inteligjencës artificiale përdoret gjerësisht në të gjithë fushat dhe shkencën në veçanti. Disa zbatime të profilit të lartë janë: motorët e përparuar të kërkimit në internet (Google Search), sistemet e rekomandimeve (të përdorura nga YouTube, Amazon dhe Netflix), të kuptuarit e të folurit njerëzor (si Siri dhe Alexa), makina vetë-drejtuese (Waymo), mjete gjeneruese ose krijuese (Arti Chat GPT dhe IA) dhe konkurrimi në nivelin më të lartë në lojërat strategjike (të tilla si shahu).

[3] Frank G. Hoffman, *Konflikti në shekullin 21*: *Ngritja e luftës hibride* (Virginia, Instituti Potomac *për Studime Politike), https://www.potomacinstitute.org/images/stories/publications/* potomac_hybridwa r_0108.pdf.

[4] Lufta hibride dhe sulmet kibernetike: Krijimi i dilemave ligjore dhe operacionale: Ndryshimi Global: Paqja dhe Siguria: faqe 32, nr. 3 (2020): faqe 340-341, https://doi.org/10.1080/14781 158.2020.17328.

Udhëheqësit politikë perëndimorë dhe drejtuesit strategjikë janë më të drejtë, të kujdesshëm ndaj delegimit të autoritetit të tyre vendimmarrës tek algoritmet e inteligjencës artificiale që aktualisht funksionojnë më pak. Nga ana tjetër, kjo i demotivon shkencëtarët nga kërkimi i temës. Ky punim nuk synon të përshkruajë nëse perëndimi duhet ose jo të integrojë inteligjencën artificiale në nivel strategjik, në vend të kësaj, ai synon të ofrojë një agjendë të përditësuar kërkimore mbi marrëdhëniet midis inteligjencës artificiale dhe luftës hibride; ai e bën këtë duke analizuar potencialin transformues të të parës në të gjitha nivelet e luftës në kontekstin e të së dytës.

Shtjellimi i ndikimit të mundshëm transformues të inteligjencës artificiale në luftën hibride do të informonte hapat e ardhshëm që Perëndimi duhet të bëjë për të siguruar qëndrueshmërinë e arkitekturës së tij të sigurisë. Qëndrimi i kujdesshëm i liderëve perëndimorë ndaj inteligjencës artificiale nuk i pengon kundërshtarët apo konkurrentët e mundshëm që të përdorin të gjithë shtrirjen e teknologjive të tilla në dëm të Perëndimit. Për shembull, duke pasur parasysh përparimet e Rusisë dhe Kinës në inteligjencën artificiale, etikën dhe standardet e ndryshme që ato zakonisht zbatojnë në kërkim dhe zhvillim. Perëndimi duhet të sigurojë që çdo dobësi të lidhur me inteligjencën artificiale sektori i tij i sigurisë ta shohë në mënyrë gjithëpërfshirëse prandaj, kjo trajtesë (teknologjia dhe inteligjenca artificiale) ka jo vetëm implikime të rëndësishme akademike, por edhe kritike në botën reale.

Objekti ka në qendër pyetjen: Në çfarë shkalle shfaqja e inteligjencës artificiale ndikon në fenomenin e luftës hibride ? Ne mund të theksojmë se teknologjia zakonisht, mund të jetë me ndikim vetëm në nivelet më të ulëta të luftës, ndërsa inteligjenca artificiale ka implikime të nivelit strategjik për sjelljen dhe mbrojtjen kundër luftës hibride. Mund të revolucionarizojë luftën hibride pasi mund të ndryshojë ekuilibri i fuqisë midis aktorëve të luftës hibride. Kështu, në epokën e inteligjencës artificiale, risia e luftës hibride nuk kufizohet vetëm në taktika dhe operacione, por edhe më tej. Shfaqja e inteligjencës artificiale legjitimon më tej ekzistencën e konceptit të luftës hibride. Ai i jep besueshmëri disa prej supozimeve themelore të Hoffman-it mbi konfliktin modern, më parë më pak të dukshme pa pasur akses të lehtë të aktorëve në një teknologji të tillë shkatërruese.

---

[5] Strategjia e sigurisë kombëtare e RSH, https://www.mod.gov.al/images/PDF/2024/strategjia-kombetare-2024.pdf

Duke pasur parasysh potencialin shkatërrues të inteligjencës artificiale, komuniteti perëndimor punon të miratojë zgjidhjet e inteligjencës artificiale me shpejtësinë e teknologjisë dhe t'u jepet prioritet në përdorimin përgjegjshëm të tyre. Inteligjenca artificiale mund të mundësojë, por edhe të sigurojë mbrojtje kundër luftës hibride. Suksesi i kësaj të fundit varet nga fakti nëse Perëndimi e përshtat inteligjencën artificiale në kutinë e mjeteve të tij kundër luftës hibride, përmes bashkëpunimit të fortë ushtarako-civil. Shembulli është bazuar në skuadrën e përshpejtimit të inovacionit të mbrojtjes të Organizatës së Traktatit të Atlantikut të Veriut (NATO) (DIANA).

1. Inteligjenca artificiale dhe konflikti

Ndërsa origjina e termit "inteligjencë artificiale" mund të gjurmohet në vitin 1956, kur shkencëtari kompjuterik John Mc Carthy e prezantoi atë në një konferencë, inteligjenca artificiale mori vrull vetëm pas viteve 1990. Në vitet 1970 dhe 1980, inteligjenca artificiale duhej t'i mbijetonte të ashtuquajturit "dimër" të inteligjencës artificiale, kur kërkimet në terren ishin të kufizuara për shkak të mungesës së fuqisë llogaritëse për ta mbështetur atë. Sidoqoftë, interesi për inteligjencën artificiale u rrit me avancimin në aftësitë e mësimit dhe përpunimit të makinerive. Megjithatë, duhej të kalonin vite përpara se aplikacionet e bazuara në inteligjencën artificiale të bëheshin të aksesueshme për fuqinë më të madhe punëtore jashtë komunitetit të ekspertëve të shkencës kompjuterike. Kjo ka ndodhur vetëm kohët e fundit për shkak të kostove më të ulëta të harduerit, kompjuterit cloud dhe aksesit të lehtë në mësimin në internet. Mundësia gjithnjë e më demokratike në edukimin e inteligjencës artificiale nuk do të thotë se të gjitha çështjet themelore të lidhura me inteligjencën artificiale janë zgjidhur.

Përkundrazi, mbeten shumë pyetje të pazgjidhura, kritike për rritjen e fushës, si: Si të rritet shpjegueshmeria dhe interpretueshmëria e zgjidhjeve të bazuara në inteligjencën artificiale? Si të sigurohet qëndrueshmëria dhe siguria e sistemeve të inteligjencës artificiale? Si të adresohen shqetësimet etike dhe të zbuten paragjykimet në teknologjinë e inteligjencës artificiale? Si të mbrohen të dhënat e përdoruesit dhe të sigurohet privatësia në sistemet e inteligjencës artificiale? Si të përcaktohet niveli i duhur i autonomisë për sistemet e inteligjencës artificiale? etj.

Të gjitha këto pyetje fitojnë dukshëm më shumë peshë nëse merret parasysh përdorimi i inteligjencës artificiale për qëllime të sigurisë. Ndërkohë, inteligjenca artificiale është në të njëjtin nivel me inteligjencën njerëzore, ndërsa super inteligjenca artificiale tejkalon talentin njerëzor. Gjendja aktuale e kërkimit dhe zhvillimit të inteligjencës artificiale mund të përshkruhet në nivelin e ngushtë të saj.

ChatGPT, është një chatbot i inteligjencës artificiale që funksionon që nga nëntori 2022. Aplikacioni, i cili ofron ndihmë dhe informacione për biseda, fitoi vëmendjen në mbarë botën për shkak të përgjigjeve të tij të artikuluara mirë. Për shembull, në përgjigje të kërkesës "Përmblidheni në 75 fjalë ose më pak ndikimin e inteligjencës artificiale në konfliktin modern", ChatGPT gjeneroi: "Inteligjenca artificiale ka një ndikim të rëndësishëm në konfliktin modern, duke përfshirë luftën kibernetike, mbledhjen e inteligjencës, armët autonome, analitiken parashikuese, sistemet e komandës dhe kontrollit, operacionet e informacionit, logjistikën dhe trajnimin. Ai mundëson sulme dhe mbrojtje të automatizuar, përmirëson vendimmarrjen, parashikon rezultatet, manipulon informacionin, i jep siguri dhe besim logjistikës dhe ndihmon trajnimin. Megjithatë, shqetësimet dhe rreziqet etike, si pasojë e paqëllimshme, si dhe llogaridhënia në sistemet autonome duhet të adresohen përmes rregullimit dhe përdorimit të përgjegjshëm."

Për të gjeneruar rezultatet në këtë nivel të sofistikuar, aplikacioni analizoi njohuritë specifike të domenit, zhargonin e industrisë dhe ndjenjat, duke kaluar nëpër sasi të mëdha informacioni mbi temën tradicionalisht, kjo kërkon një kohë të konsiderueshme kërkimi. Në të vërtetë, ka shumë informacione, disa prej tyre në formën e literaturës akademike, mbi marrëdhëniet e inteligjencës artificiale me konfliktin, megjithatë, disa tema marrin më shumë vëmendje se të tjerat, p.sh, shumë studiues e kanë lidhur inteligjencën artificiale me diskutimet dhjetëra vjeçare mbi revolucionin në çështjet ushtarake.[6]

Ndërkohë, të tjerë thellohen në aplikimet specifike ushtarake të inteligjencës artificiale në fushat e modelimit dhe simulimit.[7] Lufta kibernetike dhe dezinformimi i mundësuar janë mbuluar gjerësisht nga inteligjenca artificiale. Lidhur me studimet e rasteve sipas vendit, inovacioni ushtarak kinez ka qenë një temë tërheqëse,[8] ndërkohë që ekzistojnë shumë literatura për marrëdhëniet midis inteligjencës artificiale dhe konfliktit në përgjithësi por, çuditërisht ka pak përpjekje kërkimore mbi ndikimin e inteligjencës artificiale në luftën hibride.

---

[6] Kenneth Payne*, Inteligjenca artificiale: Një revolucion në çështjet strategjike?,*" neni 60, nr. 5 (2018): f. 7-32, https://doi.org/10.1080/00396338.2018.1518374; *Vala e gjashtë RMA;* Thornton dhe Miron*, Drejt Revolucionit të tretë.*

[7] Paul K Davis dhe Paul Bracken*, Inteligjenca artificiale për lojëra luftarake dhe modelim,* Journal of Defense Modeling and Simulation*: Applications, Methodology, Technology Special Issue Article (2022): 1-16, https://doi.org /10.1177/15485129211073126;* Simulation Methodology Development for Vibration Test of Bus Body Structure Code AIS-153:2018.

2. Inteligjenca artificiale, lufta hibride dhe kibernetika

Epoka digjitale ka sjellë spektrin e luftës kibernetike, aktorë shtetërorë dhe joshtetërorë të aftë për të orkestruar sulme ndaj infrastrukturës kritike dhe sistemeve të informacionit. Lufta kibernetike përfaqëson një ndryshim ku sulmet kibernetike të padukshme mund të kenë pasoja të prekshme dhe shkatërruese. Këto kërcënime nuk kufizohen në sferën digjitale, por shpesh manifestohet në forma hibride, duke kombinuar taktikat kibernetike me metodat konvencionale dhe jokonvencionale. Lufta hibride mjegullon linjat midis konfliktit tradicional dhe taktikave subversive, duke paraqitur një sfidë unike për sigurinë euroatlantike. Lufta kibernetike përfshin përdorimin e sulmeve digjitale nga aktorë shtetërorë ose joshtetërorë për të prishur, dëmtuar ose shkatërruar infrastrukturën kritike të një vendi ose për të depërtuar dhe vjedhur informacion.

Kjo formë e luftës është bërë një mjet i zgjedhur për shumë aktorë për shkak të kostos së ulët, mohimit dhe potencialit për ndikim të rëndësishëm. Sfidat kryesore në fushën kibernetike përfshijnë cenueshmerinë e infrastrukturës, sofistikimin e sulmeve dhe operacionet e informacionit. Infrastruktura kritike, duke përfshirë rrjetet e energjisë, sistemet financiare dhe kujdesin e shërbimeve shëndetësore, është gjithnjë e më shumë e ndërlidhur dhe e varur nga teknologjitë digjitale. Kjo ndërlidhje, megjithëse është e dobishme për efikasitetin dhe funksionalitetin, paraqet gjithashtu dobësi që kundërshtarët mund ta shfrytëzojnë për të shkaktuar dëme.

Teknikat e përdorura në luftën kibernetike po bëhen më të sofistikuara, duke përfshirë kërcënime të avancuara të vazhdueshme, ransomware[9] dhe hakerime të sponsorizuara nga shteti. Sulmet e sofistikuara mund të anashkalojnë masat tradicionale të sigurisë kibernetike, duke bërë zbulim dhe mbrojtje më sfiduese. Përtej synimit të infrastrukturës fizike, kundërshtarët përdorin operacionet kibernetike për të manipuluar informimin, përhapja e dezinformatave dhe minimi i besimit të institucionit. Këto operacione synojnë për të ndikuar në opinionin publik, për të mbjellë përçarje dhe për të destabilizuar shoqërinë nga brenda.

---

[8] Elsa B. Kania*, Ngritja e Kinës në inteligjencën artificiale dhe e ardhmja aftësitë ushtarake.* Uashington, DC, Qendra për një siguri të re amerikane. 2017, http://www.jstor.com.

[9] Ransomware është një lloj malware që mban peng të dhënat e ndjeshme ose pajisjen e viktimës, duke kërcënuar se do ta mbajë të kyçur ose më keq, nëse viktima nuk i paguan një shpërblim sulmuesit.

Kërcënimet hibride kombinojnë taktikat ushtarake dhe joushtarake, operacionet kibernetike dhe dezinformimi për të arritur objektivat strategjikë pa u përshkallëzuar në luftë të hapur. Këto kërcënime janë krijuar për të shfrytëzuar zonën gri mes paqes dhe luftës, duke e bërë të vështirë për të synuar kombet dhe aleancat për t'iu përgjigjur në mënyrë efektive.

Strategjitë e luftës hibride shpesh përfshijnë veprime të paqarta që komplikojnë atributin dhe përgjigjet. Përdorimi i forcave Proxy, mercenarëve kibernetikë dhe operacioneve të fshehta krijon mohim të besimit, duke penguar kundërmasat efektive.

Kërcënimet hibride janë krijuar për të pasur një ndikim psikologjik, duke minuar besimin në institucionet qeveritare dhe shoqëritë destabilizuese. Përdorimi i propagandës, dezinformimit dhe sulmet kibernetike ndaj objektivave civilë synojnë të gërryejnë besimin dhe kohezionin brenda dhe midis kombeve.

Adresimi i sfidave të paraqitura nga lufta kibernetike dhe kërcënimet hibride kërkojnë një qasje të shumanshme që rrit elasticitetin në nivel euroatlantik. Kombet dhe aleancat duhet të investojnë në teknologjitë e avancuara të sigurisë kibernetike, të zhvillojnë doktrinat e mbrojtjes kibernetike dhe të rrisin shkrim-leximin e sigurisë kibernetike në popullatat e tyre. Partneritetet janë thelbësore për mbrojtjen e infrastrukturës kritike dhe ndarjen e inteligjencës së kërcënimeve. Lufta kundër dezinformimit dhe propagandës kërkon përpjekje për të promovuar edukimin mediatik, të mbështesin gazetarinë e pavarur dhe të zhvillojnë aftësitë për të identifikuar dhe luftuar me shpejtësi mashtrimet. Bashkëpunimi midis vendeve dhe brenda aleancave janë thelbësore për efektin kundër kërcënimeve hibride. Kjo përfshin ndarjen e inteligjencës, koordinimin e përgjigjeve ndaj incidenteve dhe vendeve mbështetëse që janë objektiva të sulmeve kibernetike dhe të luftës hibride.

3. Çfarë mundëson inteligjenca artificiale për luftën hibride

Kur zgjerohet kjo fushë kërkimore, do të ishte e dobishme të niseshim nga tema që mbulohen në një masë më të madhe nga literatura ekzistuese. Studiuesit, të cilët shkruajnë mbi marrëdhëniet midis luftës hibride dhe inteligjencës artificiale, fokusohen kryesisht në mënyrën se si e para mundëson të dytën.[10] Ekzistojnë dy mekanizma të dukshëm se si inteligjenca artificiale mundëson luftën hibride. Të dyja janë të lidhura me zhvillimin dhe shfrytëzimin e aftësive. Së pari, inteligjenca artificiale u ka mundësuar operatorët ushtarakë të shfrytëzojnë më mirë aftësitë tradicionale që i paraprijnë kësaj fushe. Funksionet individuale të këtyre aftësive mbeten të njëjta, por algoritmet këshillojnë se si të përdoren aftësitë e ndryshme së bashku për të krijuar sinergji.

---

[10] Thiele, *Inteligjenca artificiale një mundësi kyçe e luftës hibride*.

Me fjalë të tjera, inteligjenca artificiale mundëson një qasje të zgjeruar të armëve të kombinuara në luftë. Për Hoffman, kryerja e operacioneve të tilla multimodale është një tipar përcaktues i luftës hibride. Duke analizuar me shpejtësi sasitë e mëdha të të dhënave shumëdimensionale në lidhje me mjedisin operacional, inteligjenca artificiale mund të sugjerojë se çfarë kombinimi masash në instrumentet e ndryshme të pushtetit premton rezultatin më të mirë të mundshëm, p.sh., algoritmet mund të rekomandojnë kohën më të mirë në mbështetje të një ofensive.

Pra, aftësitë tradicionale dhe instrumentet e pushtetit në të gjitha fushat mund të kombinohen dhe të bëhen më të sakta. Ndërsa këto aftësi, në vetvete, nuk janë të reja, ato janë shtuar, gjë që mund të rezultojë në ndryshime statistikash të rëndësishme në teatrin e operacioneve. Kjo ka krijuar koncepte të tilla si lufta kibernetike e mundësuar nga inteligjenca artificiale.

Së dyti, inteligjenca artificiale ka krijuar gjithashtu aftësi krejtësisht të reja operacionale që mund të shtohen në portofolin e instrumenteve të luftimit dhe të rrisin më tej multimodalitetin e luftës. Hoffman, argumenton se: "lufta hibride është një përzierje e metodave të ndryshme luftarake të rregullta por edhe të parregullta dhe pa dyshim, inteligjencës artificiale mund t'i ofrojë një sërë mundësish për të kryer këtë të fundit". Për shembull, ka një përhapje në rritje të sistemeve të armëve autonome të aktivizuara me inteligjencën artificiale (AWS) siç janë dronët. Lufta ruse kundër Ukrainës ka treguar se si këto AWS mund të përdoren për luftë të parregullt, me Kremlinin duke përdorur dronë kamikazë kundër qytetit Kiev. Një shembull tjetër është prodhimi i videove të rreme për qëllime propagandistike. Për shembull, dyshohet se Rusia synonte të qarkullonte një video të rreme të Presidentit Zelenski ku dorëzohet, për të demoralizuar forcat ukrainase.[11] Ndërsa këto përpjekje ruse nuk sollën rezultatet e pritura, ato aftësi të reja teorikisht mund të jenë një ndryshim i lojës. Më konkretisht, studiuesit argumentojnë se akumulimi i fitoreve taktike për shkak të këtyre kombinimeve të reja dhe aftësive të reja operacionale mund të prodhojë një efekt strategjik dhe të ndryshojë ekuilibrin e fuqisë midis subjekteve ndërluftuese.

Megjithatë, ka edhe efekte të tjera strategjike që inteligjenca artificiale mund të ketë në luftën hibride. Përtej pyetjeve që lidhen me aftësitë, ekzistojnë të paktën tre mekanizma të tjerë për këtë qëllim, të cilëve u kushtohet më pak vëmendje, të paktën në literaturën akademike perëndimore. Niveli i tyre më i ulët i popullaritetit është kryesisht për shkak të shqetësimeve etike sepse të gjitha janë të lidhura me rolin e inteligjencës artificiale në vendimmarrje. Kjo është ende një temë e ndjeshme.

---

[11] Mason Clark, George Barros dhe Kateryna Stepanenko, *Vlerësimi i fushatës ofensive Ruse*, 3 mars, Instituti për studimin e luftës, 2022, faqe 4, https://www.understandingwar.org/

Inteligjenca artificiale ul aftësinë digjitale por edhe aftësinë ndërvepruese fizike midis njerëzve. Forcat ajrore të Shteteve të Bashkuara kanë zbatuar logjistikën parashikuese për të mirëmbajtur flotën e tyre.[12] Asgjë nuk e pengon zbatimin e algoritmeve të tilla nga aktorë të tjerë, duke përfshirë kundërshtarët e mundshëm, duke u mundësuar atyre të zhvillojnë dhe mbajnë një gamë më të gjerë të aftësive vdekjeprurëse. Prandaj, edhe aktorët me burime të kufizuara nuk duhet të fokusohen vetëm në operacionet kibernetike. Në vend të kësaj, ata tani mund të vendosin më lehtë në përdorimin e luftës hibride në formën e tij më të pastër duke kombinuar armë të ndryshme luftarake. Në të vërtetë, studiuesit argumentojnë se inteligjenca artificiale mund të jetë një strategji për të kompensuar disa dobësi të lidhura me luftimin. Zbatimi i sistemeve të tilla të inteligjencës artificiale kërkon ekspertizë dhe burime, megjithatë, këto janë dukshëm më pak se i gjithë investimi i nevojshëm për gatishmërinë dhe, mund të ulin kostot e tjera në afat të gjatë. Kështu, kostoja e reduktuar e luftës hibride e mundësuar nga inteligjenca artificiale mund të ndikojë në vendimmarrjen, duke ndikuar potencialisht në zgjedhjen për të iniciuar ose për të marrë pjesë në luftën hibride.

Inteligjenca artificiale rrit mundësitë për befasi strategjike edhe gjatë luftës hibride, ndërsa inteligjenca artificiale aktuale klasifikohet si inteligjencë artificiale e ngushtë. Disa autorë argumentojnë se Perëndimi mund të ballafaqohet me një vendimmarrje strategjik të drejtuar ose të paktën të aktivizuar nga inteligjenca artificiale edhe në një periudhë afatshkurtër dhe afatmesme.[13] Kjo mund të krijojë një sfidë të rëndësishme, duke pasur parasysh të ashtuquajturën problem të kutisë së zezë ose mungesën e të kuptuarit se si inteligjenca artificiale punon dhe arrin në përfundime të caktuara. Për më tepër, inteligjenca artificiale është e ndarë nga psikologjia normale njerëzore, si mendimi në grup, paragjykimi i konfirmimit, optimizmi i tepruar dhe gjykimet e dobëta të rrezikut të luftës hibride .[14] Një objektiv kyç në doktrinat ekzistuese të bazuara në luftën hibride është të sjellë paqartësi dhe befasi. Kështu, nëse një sistem i inteligjencës artificiale i cili tashmë është i paqartë në vetvete, programohet ose trajnohet për të ndjekur atë objektiv qëllimisht, natyra e luftës hibride do të ishte cilësisht e ndryshme nga çdo skenar i kësaj lufte i drejtuar nga njeriu. Në fakt, shkencëtarët kinezë tashmë po eksperimentojnë me nivelin e paparashikueshmërisë që inteligjenca artificiale mund të sjellë në luftë duke përdorur ushtrinë.

---

[12] Thiele, *Inteligjenca artificiale, një mundësi kryesore e luftës hibride*, f. 6-8. Mazzucchi, *Teknologjitë e bazuara në inteligjencën artificiale* në konfliktin hibrid, f. 6; Payne, *Inteligjenca artificiale*, f. 7.

[13] Thornton dhe Miron, *Drejt revolucionit të tretë në* çështjet *ushtarake*; Olivier Guitta, *Lufta globale mbi inteligjencën artificiale tashmë filloi* Newsweek, 20 mars 2023, https://www.newsweek.com/global-war-over-ai-already-started-opinion-1788079.

[14] Payne, *Inteligjenca Artificiale*, faqe.10, 26.

Armët e inteligjencës artificiale mundësojnë krijimin e partneritetit strategjik, duke përfshirë aktorët shtetërorë dhe jo-shtetërorë. Për Hoffman-in, arritja e paqartësisë shpesh lidhet me përdorimin e PROXI-es. Irani ka mbështetur përpjekjet e Hezbollahut kundër Izraelit, megjithëse Teherani nuk ka qenë kurrë zyrtarisht në luftë me Izraelin. Përhapja e sistemeve të inteligjencës artificiale mund të ndihmojë në fillimin dhe ruajtjen e marrëdhënieve të tilla që zakonisht ndërtohen në bazë të përfitimeve reciproke si tregtia e armëve. Armët e bazuara në inteligjencën artificiale, të cilat janë të lira dhe rezervat e tyre nuk mund të monitorohen në krahasim me llojet e tjera të armëve, janë artikuj të shkëlqyeshëm për një shkëmbim të tillë midis aktorëve shtetërorë dhe joshtetërorë. Në mënyrë të veçantë, disa vende mund të vendosin të armatosin përfaqësuesit e tyre duke i furnizuar me aftësi të bazuara në inteligjencën artificiale që janë më shkatërruese dhe do të ishin më të rëndësishme për partneritete të tilla, por edhe në kontekstin e armëve kibernetike. Kështu, rritja e marrëdhënieve të tilla të aktivizuara nga inteligjenca artificiale mund të shkaktojë një ndryshim në ekuilibrin ndërkombëtar të fuqisë dhe, për rrjedhojë, të ketë një efekt strategjik më të fortë.

Si përmbledhje, inteligjenca artificiale vërteton shumë nga profecitë e mëparshme të Hoffman-it për luftën e ardhshme, të tilla si: kombinimi i aftësive, aksesi i lehtë në konflikt, paqartësia dhe partneritetet midis aktorëve të ndryshëm. Në fakt, në shumë raste, aftësitë e inteligjencës artificiale kanë potencialin për të shumëfishuar efektin e këtyre proceseve në mënyrë që ato të marrin implikime të nivelit strategjik. Kjo e bën luftën hibride të aktivizuar me inteligjencën artificiale cilësisht të ndryshëm nga luftës hibride të aktivizuar me teknologjinë e informacionit. Megjithatë, inteligjenca artificiale potencialisht jo vetëm që mund të mundësojë, por edhe të kundërshtojë sjelljen e luftës hibride.

Si i kundërvihet inteligjenca artificiale, luftës hibride?

Vlen të përmendet se shumë nga teknologjitë e bazuara në inteligjencën artificiale që mund të përdoren për të mundësuar luftën hibride mund të përdoren gjithashtu kundër tij. Për shembull, algoritmet e inteligjencës artificiale mund të përhapin propagandën, por gjithashtu mund ta luftojnë atë duke dalluar videot reale nga ato të rreme. inteligjenca artificiale mund t'u sigurojë aktorëve burime për të ushqyer marrëdhëniet e tyre të fshehta, por gjithashtu mund të ekspozojë rrjetet kriminale dhe terroriste që përfshihen në luftën hibride. Efekti i aftësive të inteligjencës artificiale në luftën hibride është subjektive, në varësi të operatorit të tyre. Disa teknologji të inteligjencës artificiale janë dukshëm më të dobishme për gatishmërinë operacionale kundër luftës hibride.

Së pari, sistemet e bazuara në inteligjencën artificiale mund të përmirësojnë ndjeshëm trajnimin, që është thelbësorë për të luftuar, luftën hibride. Simulatorët e mbështetur nga inteligjenca artificiale ofrojnë skenarë realistë të ushtrimeve me nivelin e duhur të kompleksitetit, i cili është i dobishëm për trajnimin. Me ardhjen e realitetit të shtuar dhe virtual, ndërfaqja e simulatorëve të tillë, po bëhet gjithashtu më e lehtë për t'u përdorur, kështu që platforma të tilla të bazuara në inteligjencën artificiale tani mund të përdoren edhe në nivelin e vendimmarrjes strategjike. Kur përballen me një fushatë të luftës hibride, vendimmarrësit, duhet të veprojnë në mënyrë fleksibël dhe dinamike. Trajnimi i një mentaliteti të tillë kërkon një mjedis të sofistikuar ushtrimesh, të cilin inteligjenca artificiale e ofron. Platformat e reja të inteligjencës artificiale u lejojnë udhëheqësve strategjikë të përjetojnë ushtrime më realiste dhe kërkuese në tavolinë, të cilat mund t'i trajnojnë ata në dhënien e drejtimit të duhur strategjik. Vlen të përmendet se inteligjenca artificiale ende nuk mund të simulojë asnjë ngjarje për të pasqyruar vërtetë realitetin.

Së dyti, inteligjenca artificiale mund t'u sigurojë vendimmarrësve një ndërgjegjësim më të mirë të situatës në rastin e luftës hibride në botën reale. Hoffman është shprehur se "për shkak të paqartësisë së luftës hibride, mundësia kritike për një mbrojtje të suksesshme kundër kësaj lufte është rritja e ndërgjegjësimit të situatës". Sfida është se sot ekziston një sasi marramendëse e të dhënave të pa strukturuara të inteligjencës, mbikëqyrjes dhe zbulimit, që kërkon koha për të përpunuar.[15] Inteligjenca artificiale ofron një zgjidhje të natyrshme për këtë problem dhe mund të kuptojë sasi të mëdha të dhënash duke identifikuar anomalitë dhe modelet. Duke përdorur algoritme automatike të njohjes së objektivave, sistemet e drejtuara nga inteligjenca artificiale mund të identifikojnë gjithashtu objektiva, duke përfshirë në nivel strategjik mjetet fluturuese.[16] Në të vërtetë, sisteme të tilla kanë implikime të nivelit strategjik, kështu që Shtetet e Bashkuara thuhet se kanë blerë një bazë të inteligjencës artificiale, sistemin e komandës dhe kontrollit për t'u marrë me mbingarkimin e informacionit dhe për të zvogëluar kohën e reagimit.[17] Platforma të tilla janë në gjendje jo vetëm të ofrojnë ndërgjegjësimin më të mirë të situatës në kohë reale, por janë gjithashtu të afta të tejkalojnë talentin njerëzor në analizën parashikuese. Sot, modelet e inteligjencës artificiale mund të parashikojnë ngjarje të lidhura me luftën hibride duke kërkuar ngjarje të rëndësishme, të tilla si blerjet e armatimeve të rënda,[18] kështu, vendimmarrësit marrin ndërgjegjësimin më të mirë të situatës dhe inteligjencën parashikuese bazuar në sistemet e inteligjencës artificiale, duke ndikuar në zgjedhjet e tyre strategjike.

---

[15] Zachary Davis, *Inteligjenca artificiale në fushën e betejës. Implikimet për parandalimin dhe surprizën*, PRISM faqe.8, 118 nr. 2, 2019, https://www.jstor.org/stable/26803234.

[16] Davis, *Inteligjenca artificiale në fushën e betejës*, faqe120.

[17] Jeffrey Kent, Asistenti digjital C2 i bazuar në inteligjencën artificiale. Marina e SHBA, 2016. https://www.navysbir.com/n16_2/N162-074.htm; Yan, *Ndikimi i inteligjencës artificiale*, faqe 8.

[18] Thiele, *Inteligjenca artificiale, një mundësi kyçe e luftës hibride*, faqe 8.

Sa më sipër, mund të thuhet se ka implikime të qarta të nivelit strategjik të futjes së inteligjencës artificiale në arkitekturën e sigurisë kundër luftës hibride. Kjo është arsyeja pse studiuesit shpesh arrijnë në përfundimin se për shkak të shfaqjes së teknologjive të inteligjencës artificiale, sjellja si dhe mbrojtja kundër luftës hibride hyn në një epokë të re. Prandaj, organizatat e sigurisë duhet të zbatojnë reforma të rëndësishme institucionale për të përdorur plotësisht potencialin mbrojtës të inteligjencës artificiale kundër luftës hibride.

Përfundime

Ndërsa RMA e mëparshme mund të ketë çuar në rezultate të pakënaqshme, inteligjenca artificiale mund të transformojë luftën, veçanërisht luftën hibride, duke e përfshirë në nivelin strategjik.

Së pari, ajo mundëson luftën hibride në kontekstin e aftësive operacionale dhe vendimmarrëse. Në mënyrë të veçantë, sistemet e inteligjencës artificiale mund të përmirësojnë ndjeshëm luftën multimodale, një tipar përcaktues i luftës hibride, duke analizuar se: cili kombinim i aftësive tradicionale do të japë rezultatin më të mirë në çdo mjedis operacional?. Inteligjenca artificiale ka krijuar gjithashtu aftësi të reja, veçanërisht për luftën e parregullt, e cila është një pjesë e brendshme e luftës hibride. Për shkak të këtyre kombinimeve të reja dhe armëve të luftës, forcat mund të arrijnë një nivel të paarritshëm më parë të sinergjive taktike dhe operacionale, të cilat mund të ndikojnë në mënyrë indirekte në rrjedhën strategjike të një konflikti. Inteligjenca artificiale gjithashtu mund të ndikojë drejtpërdrejt në vendimmarrjen strategjike.

Inteligjenca artificiale ul koston e luftës hibride dhe, në këtë mënyrë, e bën më të lehtë vendimin për t'u përfshirë në një konflikt të tillë. Sistemet e inteligjencës artificiale mund të përmirësojnë gjithashtu elementin e befasisë strategjike dhe të mundësojnë partneritete strategjike pasi armët e inteligjencës artificiale mund të jenë një mjet i shkëlqyeshëm për tregtimin e armëve. Të gjitha këto mekanizma të lidhura me aftësitë dhe vendimmarrjen, ishin pjesë e kuadrit origjinal të Hoffman.

Së dyti, sistemet e bazuara në inteligjencës artificiale mund të kundërshtojnë gjithashtu luftën hibride. Kjo është për shkak të shfaqjes së ushtrimeve të aktivizuara nga inteligjenca artificiale dhe ndërgjegjësimit të situatës. Në ditët e sotme, simulimet e drejtuara nga inteligjenca artificiale janë shumë më komplekse dhe mund të ofrojnë skenarë më realistë në luftën hibride. Në të njëjtën kohë, platformat e trajnimit kanë gjithashtu një ndërfaqe më të aksesueshme, e cila lejon pjesëmarrjen e vendimmarrësve strategjikë. Një inteligjencë e tillë mundëson një vendimmarrje më të mirë strategjike, veçanërisht gjatë luftës hibride në botën reale, ku duhet të identifikohen modelet e fshehura dhe sjelljet anormale në një mjedis dërrmues informacioni. Duke kuptuar natyrën shkatërruese të inteligjencës artificiale, NATO ka ndërmarrë disa iniciativa, si DIANA, që synojnë adoptimin e inteligjencës artificiale me shpejtësinë e teknologjisë.

Oficerët ushtarakë dhe politikbërësit vlerësojnë se teknologjitë e inteligjencës artificiale krijojnë luftën hibride cilësisht të ndryshme. Edhe nëse, në fillim të shekullit të 21-të, dikush mund të kishte thënë se: lufta hibride nuk është një fenomen krejtësisht i ri dhe se ka shumë referenca historike për konfliktet multimodale, shfaqja e inteligjencës artificiale dhe aplikimet e saj të sigurisë ndryshojnë narrativen. Kjo do të thotë, teknologjitë e inteligjencës artificiale çojnë në më shumë paqartësi në fushën e betejës dhe sinergji midis aktorëve dhe aftësive të ndryshme. Kështu, risia e luftës hibride nuk kufizohet në nivelet më të ulëta të luftës. Për të kapur këtë ndryshim cilësor dhe për të tërhequr vëmendjen e politikbërësve, literatura mbi lidhjen e luftës hibride me inteligjencën artificiale mund të përfitojë nga promovimi i konceptit të luftës hibride të aktivizuar me inteligjencë artificiale.

Për ta bërë këtë koncept më rigoroz, nevojiten më shumë studime, kërkimi vijues mund të marrë në konsideratë se si teknologjitë specifike të aktivizuara me inteligjencën artificiale, të tilla si llogaritja kuantike dhe shtytja e re, ndikojnë në mënyrat e ndryshme të luftës hibride. Për të lidhur përpjekjet akademike me ato të politikave, studimet duhet të eksplorojnë gjithashtu nivelin e bashkëpunimit ndërinstitucional, veçanërisht midis NATO-s dhe BE-së, në lidhje me luftën kundër luftës hibride, të mundësuar nga inteligjenca artificiale.

Bibliografia

1. Strategjia e sigurisë kombëtare 2024.
2. Strategjia ushtarake.
3. Plani afat gjatë i zhvillimit 2030.
4. NATO, *Aleatët ndërmarrin hapa të mëtejshëm për të krijuar fondin e inovacionit të NATO-s*, 20 mars 2023, https://www.nato.int/cps/en/natohq/news_213002.htm.
5. NATO, *Përmbledhje e strategjisë së inteligjencës artificiale të NATO-s*, 22 tetor 2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

6. Zachary Davis, “Inteligjenca artificiale në fushën e betejës. Implikimet për parandalimin dhe surprizën,“ PRISM (2019): 118, https://www.jstor.org/stable/26803234.
7. Davis, *Inteligjenca artificiale në fushën e betejës*.
8. Jeffrey Kent, *Asistenti digjital C2 i bazuar në inteligjencën artificiale* (Marina e SHBA, 2016) https://www.navysbir.com/n16_2/N162-074.htm; Yan, *Ndikimi i inteligjencës artificiale.*
9. Mazzucchi, teknologjitë e bazuara në inteligjencën artificiale në konfliktin hibrid; Șușnea dhe Buță, Inteligjenca Artificiale në Luftën Hibride.
10. Yan, *Ndikimi i inteligjencës artificiale*.
11. James Sharp et al., Robustness of Artificial Intelligence for Hybrid Warfare (Bruksel, Organizata e Shkencës dhe Teknologjisë së NATO-s, 2021), https://reports.nlr.nl/items/4689cd25-a934-4d83-971b- f5077e4574b4.

Ndërveprimi i fuqisë ajrore me inteligjencën ushtarake dhe sfidat e sigurisë

Major Sonila VARFI
Specialist në Drejtorinë e Radiozbulimit, AISM

Trajtesë e shkurtuar.
Në këtë artikull analizohet ndërveprimi midis fuqisë ajrore dhe Inteligjencës Ushtarake në kontekstin e mjedisit aktual të sigurisë. Duke përdorur një qasje ndërdisiplinore, përfshirë analizën e doktrinave ushtarake, strategjitë e Forcave Ajrore, strategjitë e inteligjencës ushtarake teknologjitë e Inteligjencës Artificiale dhe zhvillimet aktuale në fushën e sigurisë globale, artikulli synon të identifikojë dhe të analizojë sfidat dhe mundësitë që shfaqen nga ndërveprimi i këtyre komponentëve të rëndësishëm në arenën e sigurisë. Studimi është bazuar në shqyrtimin e të dhënave dytësore dhe analizën e përmbajtjes së literaturës së gjerë teorike mbi rastet studimore dhe shembujve të praktikës nga historia dhe aktualiteti. Gjithashtu, do të shqyrtohen sfidat emergjente dhe tendencat në fushën e veprimit të Forcave Ajrore dhe inteligjencës ushtarake, duke adresuar çështje si ndërveprueshmëria, sistemet ISR, roli i teknologjisë së informacionit dhe komunikimit.Si bazë për mbledhjen e të dhënave kam përdorur qasjen pozitiviste duke hulumtuar, botime nga media prestigjioze, të njohura në mbarë botën për seriozitetin dhe shumëllojshmërinë e materialeve. Përfundimet do të ofrojnë një kuptim të thellë të ndikimit të ndërveprimit midis Fuqisë së Forcave Ajrore dhe inteligjencës ushtarake në mjedisin aktual të sigurisë dhe se si do të ofrojnë rekomandime për politikën dhe praktikën e sigurisë në të ardhmen.

Fjalë kyçe: Inteligjenca ushtarake; fuqia ajrore; mjedisi asimetrik i sigurisë; lufta hibride; koncepti i “zonës gri”; inteligjenca artificiale; SIGINT; ISR (Intelligence, Surveillance and Reconnaissance)

Hyrje

> *Të mos kesh një forcë ajrore të përshtatshme në gjendjen aktuale të botës do të thotë të komprometosh themelet e lirisë dhe pavarësisë kombëtare. Fuqia ajrore mund t'i japë fund luftës ose t'i japë fund qytetërimit.*
>
> Winston Churchill

Fuqia ajrore dhe inteligjenca ushtarake janë dy komponentë kyçe për kapacitetet ushtarake të një vendi. Ndërveprimi i tyre përmirëson aftësinë për të zbuluar, monitoruar dhe reaguar ndaj sfidave komplekse të sigurisë, duke përfshirë kapacitetet e detektimit dhe zbulimit. Kjo lidhje e ka zanafillën që në fillimin e përdorimit të aviacionit për qëllime ushtarake. Në Luftën e Parë Botërore, aviacioni fillimisht u përdor për zbulim ajror. Në vitin 1915, anglezët kishin 48 avionë zbulimi në Francë, të cilët kryenin vëzhgime dhe raportonin lëvizjet e kundërshtarit. Kontrolli i hapësirës ajrore është thelbësor për sigurinë dhe mbrojtjen e kufijve, duke ndikuar në arenën gjeopolitike dhe fatin e vendeve.

Lufta hibride dhe ajo asimetrike përbëjnë sfida për paradigmat tradicionale të sigurisë globale. Ndërsa lufta hibride kombinon mjete konvencionale dhe jokonvencionale, lufta asimetrike përdor strategji jo të zakonshme për të përballuar kundërshtarët e fuqishëm. Fuqia Ajrore ofron fleksibilitet dhe reagim të shpejtë për kërcënimet hibride dhe asimetrike. Fuqia ajrore po kalon një fazë modernizimi për t'iu përshtatur sfidave të mjedisit ushtarak aktual. Demokratizimi i fuqisë ajrore dhe hapësinore lejon shumë kombe të kenë aftësi të fuqishme ajrore[1]. Përdorimi i Inteligjencës Artificiale (IA) ka potencial për të përmirësuar efikasitetin, precizionin dhe sigurinë e operacioneve.

Barrierat po pakësohen. Superioriteti ajror[2] është më i vështirë për t'u arritur për shkak të SAM-ve të avancuara dhe dronve të vegjël. Kostoja e zhvillimit të programit hapësinor dhe vendosjes së satelitëve në orbitë po bie, duke lejuar më shumë kombe të operojnë në hapësirë.

Inteligjenca, Mbikëqyrja dhe Zbulimi (ISR) janë komponentë kritikë të fushatës së përbashkët ushtarake[3]. Teknologjia e avancuar në dronë, satelitë dhe rrjete komunikimi përmirëson qasjen në informacion strategjik dhe inteligjencë. ISR shfrytëzon arritjen, perspektivën, shpejtësinë dhe fleksibilitetin e Fuqisë Ajrore[4].

---

[1] Tami Davis Biddle, *Air Power and Warfare: A Century of Theory and History,* Strategic Studies Institute and U.S. Army War College Press March 2019.

[2] https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/ukraine-air-war-examined-a-glimpse-at-the-future-of-air-warfare/ By Tyson Wetzel.

[3] Sanu Kainikara, *The Future Relevance of Smaller Air Forces.*

[4] Air Force Doctrine Publication 2-0, Intelligence. 1 June 2023.

Në Shqipëri, bashkëpunimi midis Forcave Ajrore dhe Inteligjencës Ushtarake është i rëndësishëm për përballimin e kërcënimeve asimetrike. Pozicioni gjeostrategjik kërkon një ndërveprim të fortë për të siguruar një përgjigje efektive dhe të koordinuar ndaj këtyre sfidave.

1. Kuptimi dhe shpërndarja e fuqisë ajrore në mjedisin asimetrik dhe hibrid të sigurisë

Fuqia ajrore është thelbësore në një mjedis asimetrik të sigurisë, duke ofruar fleksibilitet dhe modernizim në përballimin e sfidave. Kjo përfshin përdorimin e teknologjive të fundit dhe një qasje të hapur ndaj inovacionit. Kombinimi i aftësive mbështetëse dhe aftësive për operacione të pavarura vendimtare është një tipar kyç i filozofisë moderne të forcave ajrore[5].

Përdorimi i teknologjive të avancuara dhe strategjive të reja për të projektuar forcën dhe ndikimin e tyre, si dhe kontrolli i spektrit elektromagnetik, janë kyçe për efikasitetin operacional. Qasja e integruar me forcat ajrore aleate dhe sistemet e mbrojtjes ajrore dhe raketore përmirëson koordinimin dhe efikasitetin e operacioneve.

Fuqia ajrore dhe hapësinore ofron avantazhe të mëdha, duke lejuar reagim të shpejtë, fleksibilitet dhe aftësi për të vepruar në distanca të mëdha. Kjo fuqi është kritike për luftën moderne, duke ofruar ndërgjegjësim për situatën, angazhim të saktë, mbështetje logjistike dhe parandalim strategjik. Këto avantazhe luajnë një rol vendimtar në suksesin dhe sigurinë e operacioneve ushtarake të një kombi.

Në mjedise me rrezik të lartë, duke përfshirë situata asimetrike dhe konflikte hibride, forcat ajrore zhvillojnë aftësi për të ruajtur efikasitetin e tyre. Këto tipare theksojnë përqasje të avancuar ndaj teknologjisë, integrimit të fortë me aleatët dhe përshtatshmërinë ndaj sfidave të luftës moderne.

Balanca e fuqisë ajrore në Evropë ndikohet nga aftësitë e kombeve individuale, marrëveshjet e mbrojtjes kolektive, përparimet teknologjike dhe dinamikat gjeopolitike. Fuqia ajrore e NATO-s është një element kyç i mbrojtjes kolektive dhe sigurisë në rajonin trans-atlantik, duke përfshirë një gamë të gjerë të pajisjeve ajrore dhe infrastrukturës së lidhur.[6] Komanda ajrore aleate e NATO-s në Gjermani, siguron komandën dhe kontrollin e misionit të integruar të mbrojtjes ajrore dhe raketore të NATO-s. Qendrat e operacioneve ajrore në Spanjë dhe Gjermani luajnë një rol të rëndësishëm në koordinimin e operacioneve ajrore dhe në mbrojtje të hapësirës ajrore rajonale.

---

[5] Benjamin S. Lambeth, *The role of air power going into the 21ST Century.*

[6] Viktoriya Fedorchak*, Understanding Contemporary Air Power,* 1st Edition.

Forcat ajrore të shteteve anëtare të NATO-s përbëjnë fuqinë ajrore të aleancës në Evropë, duke përfshirë avionë luftarakë modernë, helikopterë luftarakë, sisteme të mbrojtjes ajrore dhe raketore, dronë dhe pajisje të tjera. Përveç NATO-s, vendet evropiane krijojnë aleanca dhe partneritete ushtarake për të rritur aftësitë e tyre të fuqisë ajrore.

Përparimet në teknologjinë e aviacionit, si aftësitë *stealth*, municionet e drejtuara me saktësi dhe sistemet ajrore pa pilot ndikojnë në balancën e fuqisë ajrore në Evropë. Vendosja e sistemeve të mbrojtjes ajrore dhe faktorët gjeopolitikë, si tensionet me rajonet fqinje, gjithashtu formatojnë këtë balancë.

Në përgjithësi, balanca e fuqisë ajrore në Evropë është një ndërveprim kompleks i faktorëve ushtarakë, teknologjikë dhe gjeopolitikë, me NATO-n dhe kombet individuale që përshtaten vazhdimisht për të ruajtur parandalimin dhe sigurinë në rajon.[7]

1.1. Ndikimi i koncepteve të luftës asimterike dhe hibride në fuqinë ajrore

Fuqia ajrore është thelbësore në konfliktet moderne, duke ofruar zbulim, sulme precize, mbështetje tokësore dhe koordinim operativ.[8] Avancimet në teknologji, si dronët dhe avionët inteligjentë, rrisin kontrollin dhe efektivitetin e operacioneve ajrore. Në konfliktet asimetrike, fuqia ajrore përdor zbulimin dhe sulmet precize për të identifikuar dhe neutralizuar kërcënimet, duke minimizuar dëmet kolaterale dhe duke ruajtur mbështetjen publike.

Përdorimi i dronve dhe avionëve për transport, mbikëqyrje dhe mbështetje taktike rrit efektivitetin e forcave tokësore. Megjithatë, mbrojtja e avionëve nga kërcënimet e armëve të thjeshta dhe sulmet e paparashikuara, mbeten sfida kryesore. Përdorimi i UAV-ve për zbulim dhe sulme precize, koordinimi me forcat tokësore dhe partnerët ndërkombëtarë, dhe integrimi i teknologjisë së avancuar përmirësojnë efektivitetin në mjedisin asimetrik.[9]

Lufta hibride kombinon taktika konvencionale, asimetrike dhe informative për të arritur objektiva komplekse.[10] Dronët, avionët inteligjentë dhe satelitët ofrojnë mbikëqyrje dhe monitorim të zonave të konfliktit, duke informuar operacionet tokësore. Elementet kryesore të luftës hibride, përfshijnë taktika asimetrike, propagandë dhe dezinformacion, sulme kibernetike, ndërhyrje ekonomike dhe diplomatike, dhe përdorimin e forcës konvencionale.

---

[7] Enhancing NATO Air and Space Power in an Age of Global Competition a Review of the JAPCC's Joint Air and Space Power Conference 2022 By Colonel Thomas Schroll, GE AF Joint Air Power Competence Centre (2020-2022).

[8] Marc Coldfelter *"Rithinking airpower vs asymmetric enemies"*.

[9] Joe Doyle, *'Rise of the Robots?',* RAF Air Power Review 16(2), Summer 2013.

[10] Frank G. Hoffman*, Conlict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), p. 28. Shih: http://www.potomacinstitute.org/ Accessed on February 7, 2018; Frank G Hoffman, "Hybrid Warfare and Challenges," Joint Forces Quarterly, Issue 52, 1st quarter 2009.

Në përfundim, fuqia ajrore, përmes përdorimit të teknologjisë dhe strategjive të avancuara, mund të ndihmojë në përballimin e sfidave të luftës asimetrike dhe hibride, duke siguruar stabilitet dhe siguri në rajonet e prekura nga këto konflikte.

2. Inteligjenca ushtarake dhe ajo artificiale si zotërim i së ardhmes dhe ndikimi i saj në fuqinë ajrore

Inteligjenca Artificiale (IA) ka filluar të përdoret që prej viteve ‘50, por ende nuk ka një përkufizim të unifikuar. IA zakonisht i referohet aftësive të një makine për të shfaqur aftësi njerëzore si arsyetimi, planifikimi dhe kreativiteti. Megjithatë, ajo është shumë më komplekse dhe aplikimet e saj po avancojnë shpejt. Në fushën ushtarake, përdoret për planifikimin, zhvillimin e operacioneve, njohjen e elementëve të luftës hibride dhe asimetrike, parashikimin e humbjes apo fitores dhe përmirësimin e saktësisë dhe precizonit të pajisjeve ushtarake.

Aftësia për të vepruar në mjediset A2/AD[11] mbetet një nga kontributet e IA, që lidhet me zbulimin dhe parandalimin e ndërhyrje së agresionit të forcave kundërshtare në zona të caktuara brenda rajoneve tokësore, hapësirave detare dhe atyre ajrore, me qëllim përfshirjen, ekspozimin e kontrolluar dhe të reduktuar të forcave ushtarake në operacione. IA mund të korrigjojë vendimet njerëzore dhe të ndihmojë në simulimin, trajnimin e burimeve njerëzore dhe forcave operacionale. Njësitë luftarake përdorin aktualisht sisteme të pavarura për të kryer detyra të vështira, kryesisht në dhënien e zgjidhjeve ndaj skenarëve komplekse të konflikteve, në operacionet asimetrike dhe luftën hibride. [12] IA përpunon të dhënat e mbledhura nga dronët, sensorët tokësorë, detarë dhe ajrorë, duke krijuar mundësinë për një analizë më të shpejtë dhe të saktë të situatës.

IA ka ndryshuar mënyrën e operimit të Forcave Ajrore, duke automatizuar proceset e operacioneve ajrore, analizon të dhënat nga sensorët dhe radarët, zhvillon sisteme autonome ajrore. Kjo ndihmon në zbulimin e kërcënimeve, identifikimin e objekteve dhe përmirësimin e mbrojtjes ajrore. IA përdoret gjithashtu, për zhvillimin e simulimeve të avancuara dhe modeleve të fluturimit, duke përmirësuar trajnimet dhe strategjitë operative. Megjithatë, është e rëndësishme të adresohen sfidat dhe rreziqet potenciale që mund të dalin.

---

[11] A2/AD (Anti-Access/Air-Denial) - Strategji ushtarake për të kontrolluar aksesin brenda një mjedisi operativ, hyrjen dhe manovrimin e një force kundërshtare në një zonë operacionale.

[12] Msc. Roland Tashi, *Inteligjenca artificiale: përparësi, rreziqe dhe masa mbrojtëse;* Revista-Ushtarake-qershor-2023.pdf

2.1. Roli i inteligjencës tradicionale ushtarake në fuqinë ajrore: SIGINT si urë lidhëse

Fuqia ajrore dhe inteligjenca ushtarake janë dy koncepte të ngushtë të lidhura që përmirësojnë aftësitë e mbikëqyrjes, planifikimit të operacioneve dhe marrjes së vendimeve në kohë reale. Kombinimi i këtyre elementeve rrit efektivitetin e forcave ushtarake në përballimin e sfidave të sigurisë. SIGINT (Inteligjenca e Sinjaleve) është një mjet i paçmuar që ndihmon ushtritë në mbledhjen e informacionit strategjik, operacional dhe taktik. SIGINT përfshin grumbullimin, përpunimin dhe analizimin e informacionit nga sinjale elektromagnetike. Informacioni i mbledhur ndihmon në parashikimin e kërcënimeve dhe marrjen e vendimeve të shpejta dhe efektive.[13]

SIGINT ka ndryshuar falë përparimeve teknologjike dhe përfshin elementë të luftës elektronike dhe kibernetike. Avionët dhe satelitët e pajisur me pajisje SIGINT mund të kapin sinjale nga ajri, duke mbuluar zona të mëdha gjeografike. Kjo ndihmon në monitorimin e veprimtarive në zona të largëta dhe në sigurimin e informacioneve të sakta për situatën taktike dhe strategjike.[14] Megjithatë, operacionet SIGINT në hapësirën ajrore, përballen me sfida si shmangia e zbulimit nga kundërshtarët, lufta elektronike dhe menaxhimi i sasisë së madhe të dhënave të mbledhura. Për të përballuar këto sfida, është e nevojshme përdorimi i teknologjive të avancuara dhe praktikave të sigurisë operacionale.

SIGINT është vendimtar për njohjen dhe parandalimin e kërcënimeve, duke ofruar informacion të vlefshëm për planifikimin dhe luftën kundër kërcënimeve elektronike. Avionët dhe dronët me pajisje ELINT (Inteligjenca Elektronike) zbulojnë dhe analizojnë sinjalet elektronike të kundërshtarëve, duke përmirësuar mbrojtjen dhe efektivitetin e operacioneve ushtarake.[15]

2.2. Bashkëveprimi i fuqisë ajrore dhe zbulimit (ISR).

ISR është një nga pesë misionet thelbësore të qëndrueshme të forcave ajrore dhe hapësinore.[16]. Me sfidat e vazhdueshme, është e domosdoshme që udhëheqësit të shfrytëzojnë plotësisht gamën e gjerë të aftësive kombëtare së bashku me ato të shërbimeve simotra, Komunitetit të Inteligjencës (IC) dhe partnerëve tanë ndërkombëtarë. ISR u ofron vendimmarrësve një pamje të plotë të situatës në terren, në ajër, në det, në hapësirë dhe në hapësirën kibernetike.[17] Ekspertët e ISR vëzhgojnë sjelljen e armikut dhe ndjekin lëvizjet e tyre, për të mbledhur informacion të rëndësishëm për planifikimin luftarak. Komandantët në fushëbetejë përdorin aftësitë ISR për të mbledhur informacionin përkatës, duke përgjuar komunikimet, monitoruar lëvizjet dhe zhvilluar plane dhe strategji. Sistemet ISR mbledhin informacion nga burime të ndryshme, përfshirë komunikimet elektronike, optike, radar dhe imazhe infra të kuqe. Asetet për mbledhjen e të dhënave përfshijnë satelitë, sensorë, avionë pa pilot dhe pajisje të specializuara në tokë, det ose hapësirë.

---

[13] Maxwell Goldstein, *A Guide to Signals Intelligence (SIGINT), January 21, 2024*

[14] The NSA's New SIGINT Annex January 13, 2021, the National Security Agency (NSA) a redacted version

[15] https://www.magaero.com/electronic-intelligence-elint-and-its-crucial-role-in-military-aircraft 13 December 2023

[16] Brown, Jason, *Strategy for Intelligence, Surveillance, and Reconnaissance,* Air University Press, 2014

Saktësia e të dhënave ISR është kritike për sigurimin e inteligjencës me cilësi të lartë dhe për rritjen e efektivitetit të operacioneve ushtarake. Zhvillimi i teknologjisë ka rritur kërkesën për aftësitë ISR në vitet e fundit. ISR përfshin inteligjencën, mbikëqyrjen dhe zbulimin, duke synuar të sigurojë informacion për komandantët për të mbështetur vendimmarrjen dhe planifikimin ushtarak, për të alarmuar forcat miqësore ndaj kërcënimeve dhe për të identifikuar dobësitë e kundërshtarit.

Procedurat e përbashkëta të inteligjencës e bëjnë më të lehtë kuptimin e operacioneve të ndryshme të inteligjencës dhe se si ato lidhen me njëra-tjetrën. Termat inteligjencë dhe ISR shpesh përdoren në mënyrë të ndërsjellë, por dallimet e tyre janë delikate. ISR mbledh informacion dhe të dhëna të nevojshme për të përmbushur kërkesat e inteligjencës, duke prodhuar inteligjencë përmes procesit të përbashkët të inteligjencës.

2.3. Ndërveprimi i fuqisë ajrore me inteligjencën.

ISR, si një aset i përbashkët, ofron kapacitete të jashtëzakonshme për mbledhjen, analizën dhe shpërndarjen e informacioneve të inteligjencës në mbështetje të operacioneve. Kombinimi i fuqisë ajrore dhe ISR përbën një pjesë të rëndësishme të aftësive të forcave të armatosura moderne. Fuqia ajrore siguron një platformë të gjerë dhe të lëvizshme për mbledhjen e informacioneve të zbulimit, të pajisur me një gamë të gjerë pajisjesh ISR, përfshirë sensorë dhe kamera optike.

Përdorimi i avionëve të pajisur me sisteme ISR ofron një pamje të gjerë dhe të detajuar të teatrit të luftës dhe zonave të interesit.[18] Informacioni i mbledhur nga platformat ISR është baza për planifikimin dhe zbatimin e operacioneve ushtarake. Fuqia Ajrore e pajisur me ISR mund të zbulojë kërcënime potenciale dhe të monitorojë veprimtarinë e kundërshtarëve, duke lejuar marrjen e masave mbrojtëse për të zvogëluar rrezikun nga kërcënimet. Përdorimi ISR nuk kufizohet vetëm në operacionet ushtarake, por ofron mbështetje për misione humanitare dhe operacione të mbrojtjes civile, duke përfshirë identifikimin e zonave të nevojshme për ndihmë humanitare dhe monitorimin e rrjedhës së refugjatëve.

---

[17] Armed Forces Communications and Electronics Association and Intelligence & National Security Alliance, 2019 Summit: Military Service Intelligence Priorities Panel, September 24, 2019, at https://www.youtube.com/watch?v=6- I8dt2gL9A

[18] Amble, John, *"Intelligence and the Future Battlefield, with Lt. Gen. Scott Berrier,"* Modern War Institute, October 25, 2019, at https://mwi.usma.edu/mwi-podcast-intelligence-future-battlefield-lt-gen-scott-berrier/.

Ndërveprimi i Fuqisë Ajrore me inteligjencën ISR është thelbësor për suksesin e operacioneve ushtarake dhe menaxhimin e situatave komplekse, duke përmirësuar aftësinë për të parashikuar, parandaluar dhe reaguar ndaj kërcënimeve të mundshme.[19]

3. Përmirësimi i bashkëpunimit dhe ndërveprimit midis forcës ajrore dhe inteligjencës ushtarake në Shqipëri

Në mjedisin global të sigurisë së sotme, roli i bashkëpunimit mes Forcave Ajrore dhe Inteligjencës Ushtarake është gjithnjë e më thelbësor për të përballuar sfidat, përfshirë kërcënimet asimetrike. Në Shqipëri, ky ndërveprim është veçanërisht i rëndësishëm për shkak të pozicionit gjeostrategjik të vendit në Ballkan.

Përmirësimi i shkëmbimit të informacionit midis Forcës Ajrore dhe Inteligjencës Ushtarake, është një nga mënyrat kryesore për të rritur efektivitetin. Një koordinim më i mirë dhe përdorimi më i efektshëm i burimeve të inteligjencës ndihmojnë në identifikimin e kërcënimeve asimetrike dhe ofrojnë një përgjigje më të shpejtë. Krijimi i një kulture të hapur dhe bashkëpunuese, duke përfshirë specialistët e inteligjencës në stafet e Forcës Ajrore dhe anasjelltas, është thelbësor. Shfrytëzimi i teknologjive si dronët Bajraktar me softuer të integruar për transmetim *live* dhe helikopterët e pajisur me sisteme vëzhgimi ofron një avantazh të madh në operacionet ushtarake. Sensorët elektro-optik dhe infra të kuq, së bashku me teknologjitë moderne të gjetësit të rrezeve dhe emërtimit lazer, përmirësojnë saktësinë dhe efikasitetin në zbulimin dhe neutralizimin e kërcënimeve.

Të dhënat nga satelitët “Albanian 1” dhe “Albanian 2” dhe avionët e zbulimit të NATO-s “Global Hawk” ndihmojnë në prodhimin e inteligjencës me cilësi të lartë, duke ofruar mbulim të vazhdueshëm dhe informacion të rëndësishëm në lidhje me hapësirën dhe kërcënimet potenciale. Global Hawk, si sistem i zbulimit ajror pa pilot, ofron informacion në kohë reale duke përdorur IMINT, SIGINT dhe MTI.

---

[19] https://www.nationaldefensemagazine.org/articles/2023/5/1 JUST IN: Air Force Updating, Clarifying ISR Vision, By Laura Heckmann

Trajnimi i përbashkët dhe zhvillimi i aftësive të përbashkëta ndihmon në krijimin e një njohurie dhe kuptimi të përbashkët të sfidave, duke përmirësuar koordinimin dhe përgjigjen ndaj kërcënimeve asimetrike. Ndërtimi i një infrastrukture të përbashkët teknologjike dhe komunikimi për shkëmbimin e informacionit në kohë reale është gjithashtu i rëndësishëm për një përgjigje më të shpejtë dhe të koordinuar ndaj kërcënimeve.

Në një mjedis të ndryshuar të sigurisë, bashkëpunimi dhe koordinimi mes forcave ajrore dhe inteligjencës ushtarake do të përmirësojnë aftësitë për të parandaluar dhe për të reaguar ndaj kërcënimeve të emergjencës së sigurisë.

Përfundime

Bashkëpunimi midis fuqisë ajrore dhe inteligjencës ushtarake, me të dhëna të nivelit strategjik, është thelbësor për kuptimin e gjithanshëm të mjedisit operacional, i cili mundëson një reagim të shpejtë dhe efektiv ndaj kërcënimeve në mjedisin e luftës asimetrike. Koordinimi i informacionit dhe shkëmbimi i inteligjencës ndihmon në evidentimin dhe/ose zbutjen e rreziqeve të sigurisë.

Ndryshimet në mjedisin e luftës asimetrike kanë sjellë sfida të reja për Fuqinë Ajrore. Është e rëndësishme të zhvillohen strategji dhe taktika të përshtatshme për të përballuar këto ndryshime dhe për të ruajtur avantazhin ajror në konflikte moderne.

Teknologjitë e mbikëqyrjes/vëzhgimit ajrore dhe inteligjenca artificiale ofrojnë mundësi të mëdha për identifikimin dhe monitorimin e kërcënimeve, duke përmirësuar masat e sigurisë dhe aftësitë e përballimit.

Integrimi i inteligjencës artificiale në mjetet ajrore mund të rrisë aftësinë e tyre për zbulimin dhe identifikimin e kërcënimeve në kohë reale, duke optimizuar efikasitetin e operacioneve ajrore, sidomos të atyre jo kinetike.

Rekomandime

Shtetet duhet të investojnë në trajnime të përbashkëta dhe ndërveprime të personelit të Forcës Ajrore dhe Inteligjencës Ushtarake për të përmirësuar bashkëveprimin. Pavarësisht se Shqipëria nuk ka asete të mirëfillta ISR, ekziston mundësia që me blerjet e fundit të dronëve “Bayraktar” dhe helikopterëve “Black Hawk” të integrohen sensorë që përdoren për mbledhje informacioni inteligjence. Zhvillimi i teknologjive të avancuara për zbulimin dhe parandalimin e sulmeve elektronike, menaxhimin e spektrit elektromagnetike, përfshirë inteligjencën artificiale, duhet të jetë një prioritet për forcën tonë ajrore.

Shtetet duhet të thellojnë bashkëpunimin rajonal dhe ndërkombëtar për të ndarë informacionin dhe për të zhvilluar strategji të përbashkëta për të përballuar kërcënime asimetrike.

Një opsion për vendin tonë, do të ishte krijimi i një rrjeti të dhënave të mbikëqyrjes/vëzhgimit ajror dhe hapësinor që mund të përftohen jo vetëm nga asetet tona kombëtare si satelitët "Albania 1" dhe "Albania 2", dhe dronët "Bayraktar", por edhe nga sistemet e vëzhgimit dhe zbulimit si nga platformat e helikopterëve "Cougar" dhe "Black Hawk", por ashtu edhe nga radarët e vëzhgimit ajror.

Nga ana tjetër, vendi ynë mund të aplikojë në Aleancë për të marrë të dhënat e aseteve të NATO-s "Global Hawk" të stacionuar në Bazën Ajrore Sigonella në Itali dhe/ose nga burime të tjera të vendeve partnere.

Në Shqipëri, së bashku me rekomandimet e mësipërme, një hap i parë i mundësive reale është shfrytëzimi i të dhënave të dronve "Bayraktar", helikopterëve "Black Hawk" dhe Cougar për qëllime të mirëfillta inteligjence duke i pajisur me sensorë dhe pajisje për interceptimeve SIGINT, krijimi i kapaciteteve teknike dhe teknologjike për ruajtjen dhe arshivimin e të gjitha të dhënave të zbulimit të përftuara nga platformat ajrore dhe hapësinore.

Mbetet sfidë e forcës ajrore që të administrojë të gjitha këto të dhëna në servera/database përkatëse dhe e IASM për krijimin e protokolleve për mundësimin e aksesit, analizimit dhe shpërndarjes së produkteve të tyre te palët e interesuara.

Bibliografia

1. IA-r Force Doctrine Publication 2-0, Intelligence. 1 June 2023.
2. Dobbs, Thomas; Fallon, Garth; Fouhy, Sarah (9 September 2020).*Grey Zone*. The Forge (Report). *Australian Defence College*. Archived from *the original* on 8 April 2022. *Retrieved 18 March 2022*.
3. Jérôme Lespinois (de) , "Gjeopolitika e ajrit dhe fati i Evropës".
4. Tami Davis Biddle IA-r power and warfare: a century of theory and history strategic studies institute and U.S. Army War College Press March 2019.
5. The Role of IA-r Power Going Into the 21st century Benjamin S. Lambeth.
6. The Future Relevance of Smaller IA-r Forces by Sanu KIA.
7. 1st Edition, Understanding Contemporary IA-r Power, By Viktoriya Fedorchak.
8. Enhancing NATO IA-r and space power in an age of Global Competition A Review of the JAPCC's Joint IA-r and space power conference 2022 By Colonel Thomas Schroll, GE AF Joint IA-r power competence centre (2020-2022)
9. Frank G. Hoffman, conflict in the 21st Century: The rise of hybrid wars

(Arlington, VA: Potomac institute for policy studies, 2007), p. 28av AI lable at http://www.potomacinstitute.org/ Accessed on February 7, 2018; Frank G Hoffman, "Hybrid Warfare and Challenges," Joint Forces Quarterly, Issue 52, 1st quarter 2009.

10. War in Ukriane by the center for preventive action updated March 06, 2024
11. IA-r strategy and the underdog', in P. Gray (ed.), IA-r Power 21: Challenges for the New Century (London: The Stationery Office, 2000).
12. The NSA's New SIGINT Annex January 13, 2021, the National Security Agency (NSA).
13. A Guide to signals intelligence (SIGINT) Maxwell Goldstein MAXWELL GOLDSTEIN JANUARY 21, 2024.
14. Inteligjenca artificiale: përparësi, rreziqe dhe masa mbrojtëse Msc. Roland Tashi Revista-Ushtarake-qershor-2023.pdf.
15. Rand corporation, military applications of artificial intelligence, ethical concerns in an uncert IA-r World, 2020.
16. Brown, Jason, strategy for intelligence, surveillance, and recon IS science, IA-r University Press, 2014.

Burime elektronike

1. Allied IA-r Command | Home (nato.int).
2. https://defence.IA/industry-news/atlantic-council-militaries-IA/ August 15, 2023.
3. https://www.atlanticcouncil.org/content-series/IArpower-after-ukriane/ukriane-https://www.IA-r
4. andspaceforces.com/space-superiority-democratization-of-IA-r-power-are-the-future/ Sept. 21, 2022 | By Chris Gordon
5. https://www.magaero.com/electronic-intelligence-elint-and-its-crucial-role-in-military-IArcraft December 2023 Electromagnetic spectrum.
6. http://www.britannica.com/EBchecked/topic/183297/electromagnetic-spectrum (online, cit. 2015-01-10).

RUBRIKA E TRETË

ARSIMIMI DHE STËRVITJA

Mbështetja logjistike e integruar në konceptin logjistik të NATO-s

Kolonel (R) Arben DHULI

Trajtesë e shkurtuar.

Në këtë punim, kam synuar që, përmes fakteve të mbledhura nga burime profesionale të logjistikës, si nocion, të sjell në vëmendjen e lexuesit dhe kryesisht të specialistëve të fushës, risitë dhe tendencat që revolucioni teknologjik ka ofruar. Për këtë, kam analizuar termin "logjistikë e integruar", si ndryshon ajo nga logjistika tradicionale dhe se si zbatimi i suksesshëm mund t'i ndihmojë si kompanitë private, por edhe logjistikën ushtarake të NATO-s, të kenë sukses në një mjedis kompleks dhe dinamik biznesi.

Termi "logjistikë e integruar" është përdorur në vitet 1980, të cilat shënuan një pikë kthese duke theksuar nevojën për një perspektivë holistike (një qasje ndaj kërkimit shkencor që merret me studimin e sistemeve komplekse), që integron të gjitha funksionet e logjistikës për të rritur efikasitetin dhe konkurrencën. Me futjen e teknologjisë së informacionit në vitet 1990, ajo fitoi edhe më shumë mbështetje nëpërmjet analizave moderne në kohë reale dhe sistemeve të menaxhimit të të dhënave.

Në shekullin e 21-të, logjistika e integruar është bërë një pjesë e rëndësishme e strategjisë së biznesit, e njohur për aftësinë e saj për të ulur kostot, për të përmirësuar kënaqësinë e klientëve, si dhe për të forcuar konkurrencën. I zhvilluar fillimisht për qëllime ushtarake, MIL[1] *tani përdoret gjerësisht edhe*

---

[1] Military integrated logistik

në organizatat komerciale të shërbimit ndaj klientit. Qëllimi kryesor i MIL është të krijojë sisteme që zgjasin më shumë, kërkojnë më pak mbështetje dhe në fund të zvogëlojnë kostot duke rritur kthimin e investimeve.

Mbështetja e Integruar Logjistike përfshin aspekte të ndryshme të mbështetjes, jo vetëm gjatë blerjes, por edhe gjatë gjithë ciklit të jetës operacionale të sistemit. Elementet kryesore të MIL përfshijnë inxhinierinë e besueshmërisë, planifikimin e mirëmbajtjes, mbështetjen e furnizimit, fuqinë punëtore dhe personelin, trajnimin, të dhënat teknike dhe më shumë. Duke integruar këto disiplina, MIL synon të optimizojë mbështetjen e produktit dhe të ulë kërkesën për logjistikë.

Fjalët kyçe: Mbështetja e Integruar Logjistike, strategji, mbështetja tradicionale logjistike, menaxhim, planifikim, qasje holistike, plan i integruar i mbështetjes logjistike etj.

1. Mbështetja me logjistikë të integruar (MLI)

Mbështetja e Integruar Logjistike (MIL) është një qasje gjithëpërfshirëse e disiplinuar e unifikuar ndaj menaxhimit dhe aktiviteteve teknike të nevojshme që siguron mbështetje efikase për sistemet gjatë gjithë ciklit të tyre jetësor. E zhvilluar fillimisht për qëllime ushtarake, MIL tani përdoret gjerësisht edhe në organizatat komerciale të shërbimit ndaj klientit. Qëllimi kryesor i MIL është të krijojë sisteme që zgjasin më shumë, kërkojnë më pak mbështetje dhe në fund të zvogëlojnë kostot duke rritur kthimin e investimeve. Ajo përfshin aspekte të ndryshme të mbështetjes, jo vetëm gjatë blerjes, por edhe gjatë gjithë ciklit të jetës operacionale të sistemit. Elementet kryesore të MIL përfshijnë inxhinierinë e besueshmërisë, planifikimin e mirëmbajtjes, mbështetjen e furnizimit, fuqinë punëtore dhe personelin, trajnimin, të dhënat teknike dhe më shumë. Duke integruar këto disiplina, MIL synon të optimizojë mbështetjen e produktit dhe të ulë kërkesën për logjistikë.

Mbështetja e integruar logjistike[2] është planifikimi dhe veprimi i integruar i një numri disiplinash në bashkëpunim me njëra-tjetrën, për të siguruar disponimin e sistemit. Planifikimi i secilit element të MIL zhvillohet në mënyrë ideale në koordinim me përpjekjet inxhinierike të sistemit dhe me njëri-tjetrin. Mund të kërkohen shkëmbime ndërmjet elementeve në mënyrë që të fitohet një sistem që është i përballueshëm (kostoja më e ulët e ciklit jetësor), funksional, i qëndrueshëm, i transportueshëm dhe i trajtuar ndaj efekteve mjedisore. Në disa raste, një proces i dedikuar i Analizës së Mbështetjes Logjistike do të përdoret për të identifikuar detyrat brenda çdo elementi të mbështetjes logjistike.

“Mbështetja e Integruar Logjistike është një strategji menaxhimi për planifikimin dhe zhvillimin e mbështetjes efikase për sistemet gjatë gjithë ciklit të tyre jetësor. MIL mund të aplikohet në çdo moment gjatë zhvillimit të një produkti ose sistemi”.

---

[2] https://acc.dau.mil/CommunityBrowser.aspx?id=280255&lang=en-US

Ndryshimi ndërmjet Mbështetjes së Integruar Logjistike dhe Mbështetjes Tradicionale Logjistike, vihet re në dy aspekte:

- Qasja holistike (një qasje ndaj kërkimit shkencor që merret me studimin e sistemeve komplekse). Sistemet trajtohen si tërësi koherente, pjesët përbërëse të të cilave kuptohen më mirë në kontekst dhe në lidhje si me njëri-tjetrin ashtu edhe me të tërën.

MIL merr një qasje gjithëpërfshirëse, duke marrë parasysh të gjithë ciklin e jetës së një sistemi ose produkti. Ajo mbulon fazat e planifikimit, blerjes, funksionimit dhe asgjësimit. Ndërsa mbështetja tradicionale logjistike shpesh fokusohet në aspekte specifike (p.sh., transporti, menaxhimi i inventarit), pa marrë parasysh kontekstin më të gjerë.

MIL integron disiplina të ndryshme, duke përfshirë inxhinierinë e besueshmërisë, mirëmbajtjen, menaxhimin e zinxhirit të furnizimit, trajnimin dhe të dhënat teknike. Ndërsa logjistika tradicionale tenton të trajtojë funksionet individuale veçmas.

MIL i jep përparësi mbështetjes gjatë gjithë jetës së sistemit. Ajo synon të minimizojë kohën e ndërprerjes, të rrisë besueshmërinë dhe të reduktojë kostot e mirëmbajtjes. Logjistika tradicionale mund t’i japë përparësi kursimeve të kostos pa theksuar mbështetjen afatgjatë.

- Reduktimi afatgjatë i kostos. MIL synon të reduktojë kostot e përgjithshme të ciklit jetësor duke optimizuar proceset mbështetëse. Ndërsa logjistika tradicionale mund të fokusohet më shumë në kursimet afatshkurtra të kostos.

Në përmbledhje, MIL ofron një qasje holistike dhe të integruar për mbështetjen logjistike, duke theksuar efikasitetin afatgjatë. Ndërsa logjistika tradicionale priret të jetë më e fragmentuar dhe reaktive.

Po japim disa shembuj të Mbështetjes së Integruar të Logjistikës (MIL) të cilat janë:

- **Menaxhimi i inventarit vetëm në kohë**: Një strategji që minimizon nivelet e inventarit duke ofruar materiale ose pjesë saktësisht kur nevojiten, duke reduktuar kostot e magazinimit dhe mbetjet.
- **Sistemet e gjurmimit në kohë reale**: Zbatimi i teknologjive si ajo GPS për të monitoruar lëvizjen e mallrave, automjeteve ose aseteve në kohë reale.
- **Menaxhimi efikas i magazinës**: Optimizimi i paraqitjes së magazinës, vendosja e inventarit dhe proceset e përmbushjes së porosive për të rritur efikasitetin dhe për të ulur kostot.

- **Bashkëpunimi me furnizuesit**: Koordinim i ngushtë me furnitorët për të siguruar dërgesat në kohë, kontrollin e cilësisë dhe burimet me kosto efektive.
- **Optimizimi i rrugëve të shpërndarjes**: Përdorimi i analitikës së të dhënave dhe softuerit të planifikimit të rrugës për të minimizuar kohën e transportit, konsumin e karburantit dhe vonesat e dorëzimit.
- **Përdorimi i teknologjive të informacionit**: Përdorimi i sistemeve softuerike për menaxhimin e inventarit, përpunimin e porosive dhe dukshmërinë e zinxhirit të furnizimit.
- **Riciklimi dhe paketimi i qëndrueshëm**: Përfshirja e praktikave (miqësore) me mjedisin në logjistikë, të tilla si riciklimi i materialeve dhe përdorimi i paketimeve të ndërgjegjshme për mjedisin.
- **Trajnimi i vazhdueshëm i personelit**: Sigurimi që stafi i logjistikës të marrë trajnime të vazhdueshme për të qëndruar i përditësuar mbi praktikat më të mira dhe teknologjitë e reja.

Këta shembuj ilustrojnë sesi logjistika e integruar nuk është vetëm një teori strategjike, por një realitet operacional që drejton suksesin e kompanive të ndryshme në industri të ndryshme. Zbatimi efektiv i këtyre qasjeve tregon aftësinë e logjistikës së integruar për të përmirësuar efikasitetin, për të ulur kostot dhe për të forcuar pozicionin konkurrues në treg.

Kompanitë e logjistikës gjithashtu luajnë një rol të rëndësishëm në këtë skenar dhe kontribuojnë në zhvillimin e qëndrueshëm të logjistikës së integruar. Logjistika integrale jo vetëm që luan një rol vendimtar në mjedisin e sotëm të biznesit, por rëndësia e saj do të vazhdojë të rritet në mënyrë të qëndrueshme në të ardhmen.

2. Logjistika e integruar, pjesë e rëndësishme e strategjisë së biznesit

Logjistika e integruar, e cila u shfaq si një paradigmë revolucionare në menaxhimin e biznesit, ka pësuar një zhvillim të jashtëzakonshëm që nga shfaqja e saj e parë në vitet 1950. Fillimisht e fokusuar në logjistikë dhe transport, globalizimi dhe kompleksiteti i zinxhirëve të furnizimit kanë çuar në një tranzicion të qartë drejt një strategjie të integruar. Vitet 1980 shënuan një pikë kthese për termin "logjistikë e integruar", duke theksuar nevojën për një perspektivë holistike që integron të gjitha funksionet e logjistikës për të rritur efikasitetin dhe konkurrencën. Me futjen e teknologjisë së informacionit në vitet 1990, ajo fitoi edhe më shumë vrull nëpërmjet analizave moderne në kohë reale dhe sistemeve të menaxhimit të të dhënave.

Në shekullin e 21-të, logjistika e integruar është bërë një pjesë e rëndësishme e strategjisë së biznesit, e njohur për aftësinë e saj për të ulur kostot, për të përmirësuar kënaqësinë e klientëve dhe për të forcuar konkurrencën. Nga fillimet e vogla në një rol qendror në strategjitë e sotme, logjistika e integruar po shfaqet si një forcë transformuese që po evoluon vazhdimisht për të përballuar sfidat e së nesërmes. Përkufizimi i logjistikës së integruar si një qasje gjithëpërfshirëse për menaxhimin e zinxhirit të furnizimit, nga prokurimi i lëndëve të para deri te dorëzimi përfundimtar i produkteve te klientët. Të gjitha elementet logjistike, duke përfshirë transportin, magazinimin, përmbushjen dhe shpërndarjen, janë të koordinuara në mënyrë efikase, duke siguruar qetësi dhe efikasitet në çdo fazë të procesit.

Dallimi midis logjistikës dhe logjistikës së integruar është më shumë se nuanca semantike. Ai përfaqëson një ndryshim thelbësor në mënyrën se si kryhet menaxhimi i zinxhirit të furnizimit . Ndërsa logjistika tradicionale fokusohet në detyra specifike, të grimcuara, të tilla si transporti ose magazinimi, logjistika e integruar përfshin një qasje holistike. Një qasje holistike merr në konsideratë të gjithë personin, jo vetëm nevojat e tij për shëndetin mendor. Ai gjithashtu merr parasysh mirëqenien e tyre fizike, emocionale, sociale dhe shpirtërore.

Dëgjimi, pyetja dhe kontrollimi janë aftësi kyçe kur ofrohet mbështetje gjithëpërfshirëse, duke ditur se përvoja e çdo personi është unike dhe e ndikuar nga faktorë të ndryshëm si mosha, kultura dhe besimet. që kërkon të integrojë dhe optimizojë të gjitha aktivitetet. Logjistika tradicionale tenton të adresojë problemet afatshkurtra dhe aktivitetet specifike pa marrë gjithmonë parasysh marrëdhëniet dhe varësitë midis pjesëve të ndryshme të zinxhirit të furnizimit. Logjistika e integruar, nga ana tjetër, merr një perspektivë afatgjatë dhe pranon se të gjitha funksionet e logjistikës duhet të koordinohen për të përmirësuar efikasitetin e përgjithshëm. Fokusi ndaj klientit është një tjetër diferencues. Ndërsa logjistika tradicionale fokusohet më shumë në uljen e kostove operative, logjistika e integruar shkon më tej duke i dhënë përparësi përmirësimit të vazhdueshëm të përvojës së klientit.

Ne i kushtojmë vëmendje të veçantë faktorëve të tillë si koha e dorëzimit, disponueshmëria e produktit dhe aftësia për t’u përshtatur me kërkesat në ndryshim të tregut. Në praktikë, logjistika e integruar përfshin bashkëpunim të ngushtë midis departamenteve të ndryshme brenda një kompanie dhe futjen e teknologjive të avancuara. Çelësi është të pranohet se çdo element i zinxhirit të furnizimit është i ndërlidhur dhe se përmirësimi i tij do të ketë një ndikim pozitiv në performancën e përgjithshme.

Si përfundim, ndryshimi i rëndësishëm ndërmjet logjistikës tradicionale dhe logjistikës së integruar qëndron në qasjen dhe filozofinë e tyre. Kështu që Logjistika e integruar kërkon pjekurinë globale duke parë të gjithë zinxhirin e furnizimit. Ndërsa Logjistika tradicionale fokusohet në komponentë individualë. Ky ndryshim në perspektivë është thelbësor në një botë biznesi që kërkon efikasitet, fleksibilitet dhe përvoja të jashtëzakonshme të klientit. Logjistika e integruar përqendrohet në fleksibilitet, duke u mundësuar kompanive të përshtaten shpejt me ndryshimet në kërkesën e tregut duke shmangur rezervat e tepërta ose duke shmangur stoqet.

Për të krijuar një sistem logjistik gjithëpërfshirës, që plotëson nevojat e tregut të sotëm dhe është i pozicionuar në mënyrë strategjike për të përmbushur sfidat e biznesit të së nesërmes, është e nevojshme ndërthurja e objektivave të mëposhtëm:

Bashkëpunimi i brendshëm dhe i jashtëm: nxitja e bashkëpunimit të ngushtë me partnerë të jashtëm në të gjitha departamentet e kompanisë dhe në të gjithë zinxhirin e furnizimit për të promovuar komunikim efektiv dhe vendimmarrje të përbashkët.

Qëndrueshmëria: minimizimi i ndikimit mjedisor të zinxhirit të furnizimit, duke marrë parasysh praktikat e qëndrueshme të logjistikës.

Përmirësimi i vazhdueshëm: logjistika e integruar përpiqet të zbatojë një proces përmirësimi duke vlerësuar vazhdimisht operacionet dhe duke zbatuar rregulla për të ruajtur efikasitetin afatgjatë.

Integrimi efektiv i logjistikës së integruar në një kompani përfshin bashkëpunim të ngushtë midis të gjitha departamenteve që lidhen me zinxhirin e furnizimit. Zbatimi i teknologjive të avancuara të informacionit, të tilla si: softueri i logjistikës, sistemet e menaxhimit të depove dhe softueri TMS, është thelbësor për të koordinuar në mënyrë efikase operacionet. Përveç kësaj, trajnimi i stafit dhe përafrimi i objektivave të biznesit me strategjitë e logjistikës janë thelbësore për sukses.

3. Analiza e mbështetjes logjistike

Analiza e mbështetjes logjistike është kritike për rritjen e efikasitetit të mirëmbajtjes dhe uljen e kostove të mbështetjes duke planifikuar paraprakisht të gjitha aspektet e MIL. Ndikimi i logjistikës në ekonominë globale ka dy efekte mbi organizatat dhe ekonominë globale. Së pari, një kompani kryen shpenzime të shumta, një prej të cilave është kostoja e logjistikës. Këto shpenzime dhe kosto logjistike ndikojnë në vendimet ekonomike dhe anasjelltas. Së dyti, logjistika lejon shitjen e produkteve dhe shërbimeve, si dhe shërbimin e lidhur me klientët dhe një sërë operacionesh ekonomike. Shumë biznese i kushtojnë një vlerë të lartë shërbimit ndaj klientit dhe logjistika mund t'i ndihmojë ata të fitojnë një avantazh konkurrues. Një MIL i suksesshëm kërkon zbatimin e një plani të integruar të mbështetjes logjistike (PIML). Ky plan krijohet gjatë fazës së konceptit të prokurimit të sistemit dhe përditësohet gjatë gjithë ciklit jetësor të sistemit.

Më poshtë janë disa nga avantazhet e zbatimit efektiv të një plani të integruar të mbështetjes logjistike (PIML):

- Një sistem më efektiv që përdoret nga klienti gjatë gjithë jetëgjatësisë së sistemit.

- Një sistem që i përmbahet deklaratave operative dhe të kërkesave të përdoruesit gjatë gjithë ciklit jetësor të sistemit.

- Një biznes më efikas që plotëson buxhetet duke projektuar në mënyrë realiste, duke matur shpenzimet aktuale dhe duke shmangur surprizat.

- Nuk do të ketë përmirësime, modifikime apo riparime të kushtueshme në krizë si rezultat i aktiviteteve të parakohshme.

- Nëpërmjet këtij plani shmangen dështimet e kushtueshme në produktet vitale, të shtrenjta dhe që kërkojnë kohë. Gjithashtu ruajtja e të dhënave, komunikimi dhe teknologjia e informacionit (IT) kanë një rritje teknologjike në kapacitet. Sasia e dokumentacionit të prodhuar në një mjedis inxhinierik (do të mbushte ngarkesat e kamionëve nëse printohej). Për fat të mirë, në ditët e sotme, këto dokumente mund të ruhen në mënyrë elektronike.

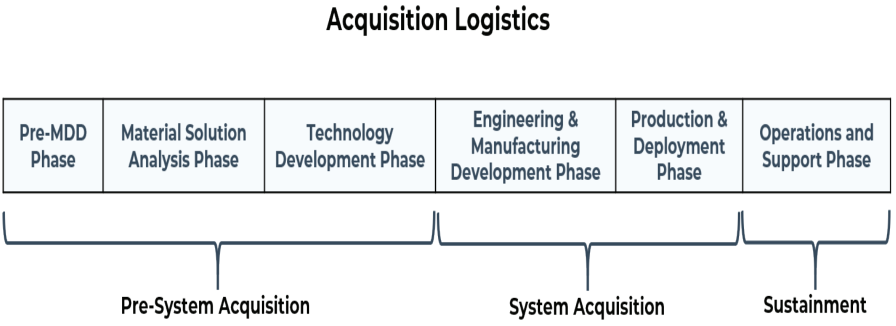
- Një mënyrë për të menduar për këtë proces është si një proces i vazhdueshëm përmirësimi i cili do të thotë se çdo detaj do të shqyrtohet dhe rregullohet mirë për të maksimizuar funksionalitetin. Kjo mund të arrihet nëprmjet përdorimit të shërbimeve të tilla si: mirëmbajtja rutinë, riparimet, kurset e trajnimit dhe testet. Pas testimit, krijohet një raport që përshkruan rekomandimet për ndryshim ose përmirësim. Ai do të identifikojë gabimet e njohura që ndërhyjnë në efikasitetin operacional, ngadalësojnë proceset dhe shkaktojnë pakënaqësi të punonjësve dhe menaxhmentit. Kjo është arsyeja pse është thelbësore për të zhvilluar kompetencat e këtyre individëve në mënyrë që ata të mund të lulëzojnë në një atmosferë me kërkesa të larta dhe me presion të lartë.

- Dy mënyra të zakonshme janë testimi psikometrik dhe/ose i aftësisë. Këto do t’ju ndihmojnë të përcaktoni personalitetin, aftësitë dhe talentet e një punonjësi. Më pas, menaxhmenti mund ta përdorë këtë informacion për të caktuar individët në role bazuar në rezultatet e këtyre vlerësimeve. Kjo është metoda më e shpejtë dhe më e drejtpërdrejtë për të zbuluar një përputhje të përsosur midis të dyjave.

Forma dhe funksionaliteti efektiv operacional i mbështetjes së produktit dhe sistemeve të shërbimit ndaj klientit varet nga mirëmbajtja rutinë. Është thelbësore në MIL që të ketë funksionim optimal të sistemit, i cili mund të arrihet përmes një plani të rregullt të përditësimit, mirëmbajtjes dhe riparimit. Kjo strategji proaktive dhe jo reaktive siguron që një sistem të jetë gjithmonë i shëndoshë operacionalisht. Kjo zvogëlon gjasat e një humbje prodhimi të shkaktuar nga një avari, ndërprerje ose mosfunksionim i sistemit. Pasojat e dështimit të pajisjeve për shkak të mungesës së mirëmbajtjes mund të jenë të rënda. Modeli tradicional i biznesit merr parasysh shpenzimet e riparimeve dhe, duke përdorur një qasje afatshkurtër, e bën këtë vetëm kur lind një problem. Marrja e një pamje afatgjatë me MIL është një procedurë afatgjatë që synon të parandalojë shfaqjen e problemeve. Ata përdorin më së miri burimet e disponueshme duke zbatuar një sërë masash mbështetëse gjatë gjithë jetës së projektimit të një produkti ose sistemi të shërbimit ndaj klientit. Shumë kompani bëjnë gabim duke u fokusuar vetëm në mbijetesën afatshkurtër. Në tregun e sotëm ultra-konkurrues, kjo mund të jetë një recetë për katastrofë. Qasja e Mbështetjes së Integruar të Logjistikës (MIL) siguron qëndrueshmërinë dhe suksesin afatgjatë të një kompanie. Programet MIL shkurtojnë mbetjet, thjeshtojnë operacionet dhe u japin punonjësve tuaj më shumë kontroll.

4. Mbështetja logjistike e blerjes

Zbatimi i strategjisë për blerjen/prodhimin e ri të materialit ofron mundësinë për të maksimizuar ndikimin e dobishëm të elementeve jo vetëm gjatë fazës së blerjes, por gjatë gjithë ciklit të jetës së tij operacionale. Mbështetja Logjistike e blerjes ka përvojë/ekspertizë në kryerjen e mbështetjes logjistike në faza të ndryshme të procesit të blerjes. Ajo përdor Kornizën e Përvetësimit të Mbrojtjes (DAF) të përshkruar më poshtë si një udhëzues për menaxhimin e programeve të blerjes së sistemit.


Acquisition Logistics
Pre-MDD Phase
Material Solution Analysis Phase
Technology Development Phase
Engineering & Manufacturing Development Phase
Production & Deployment Phase
Operations and Support Phase
Pre-System Acquisition
System Acquisition
Sustainment

Pra, tabela e mësipërme sqaron qartë se ***blerja para sistemit*** ka në vetvete si fazë të parë përzgjedhjen e materialeve (faza e analizimit) dhe fazën e zhvillimit teknologjik, ndërsa ***sistemi i blerjes*** përfshin Fazën e Zhvillimit dhe Prodhimit Inxhinierik dhe Fazën e prodhimit dhe të zhvillimit, dhe e fundit është ***mbajtja*** që përfshin operacionet dhe fazën e mbështetjes.

Procesi i planifikimit të logjistikës së blerjes përfshin një rishikim të aftësive të sistemit dhe analizën e çështjeve dhe shqetësimeve të besueshmërisë, mirëmbajtjes dhe mbështetjes së sistemit ekzistues.

• Të dhënat nga analiza përdoren për të përcaktuar strategjinë e mbështetjes dhe konceptin e mirëmbajtjes. Strategjia mbështetëse identifikon qasjen e programit për të përmbushur objektivat e logjistikës së ciklit jetësor. Koncepti i mirëmbajtjes përcakton në terma të gjerë se si sistemi do të mirëmbahet për të përmbushur objektivat e pragut të disponueshmërisë. Strategjia e mbështetjes dhe koncepti i mirëmbajtjes përbëjnë themelin e procesit të zhvillimit të mbështetjes së produktit.

• Hapi tjetër në procesin e planifikimit të logjistikës së blerjes është kryerja e anketave të tregut për të përcaktuar nëse tendencat aktuale të projektimit adresojnë përsosin më tej çështjet dhe identifikojnë tendencat e tregut ku duhet të fokusohemi. Bazuar në analizën e kryer, strategjia e mbështetjes është dedikuar për të përzgjedhur alternativën e mbështetjes me kosto efektive për sistemin dhe konceptin e mirëmbajtjes së tij.

Përfundime

- Perspektiva e së ardhmes për logjistikën e integruar në botën e biznesit po shfaqet si një mundësi kyçe e suksesit të logjistikës ushtarake kombëtare por dhe të NATO-s.

- Ndërsa kompanitë përpiqen vazhdimisht të përmirësojnë operacionet dhe të përmbushin pritshmëritë e klientëve, zbatimi efektiv i logjistikës në fund po bëhet një diferencues kryesor.

- Aftësia për të përqafuar inovacionin teknologjik, për t’iu përgjigjur sfidave mjedisore, për t’u përqendruar në përvojën e klientit dhe për të nxitur bashkëpunimin global po vendoset si një element kyç i strategjisë që ndihmon organizatat private dhe shtetërore jo vetëm të mbijetojnë, por edhe të lulëzojnë në një mjedis dinamik biznesi.

- Entet shtetërore përfshirë këtu edhe ato ushtarake edhe në këtë fushë duhet të ndjekin ritmin, idetë dhe procesin transformues teknologjik të sipërmarrjeve private, pasi ata janë në pararojë të implementimit të “logjistikës së integruar”.

Bibliografia

1. US Defense Acquisition University on Integrated Logistics Support (ILS) Elements
2. James V. Jones, *Integrated Logistics Support Handbook*, third edition.
3. United Kingdom Ministry of Defence (UK MoD) Through Life Support (TLS) - Directorate into the following elements and promulgated in UK Defence Standard (DEFSTAN) 00-600
4. “Defense Acquisition University”. *Archived from* the original *on 2009-04-*

23. Retrieved 2016-07-06 SX000i - International guide for the use of the S-Series of Integrated Logistics Support (ILS) specifications

5. Doktrina Logjistike e FARSH.
6. NATO Logistics Handbook, STANAG 2115. Njësia bazë e konsumit të karburantit (Fuel consumption unit).

Forca përmes dijes:
Roli kyç i Edukimit Ushtarak Profesional në sigurinë kombëtare të Shqipërisë

Kolonel (R) Dr. Çlirim TOCI
Kolegji i Vendeve të Baltikut, Estonia

Trajtesë e shkurtuar.

Në një botë që ndryshon me shpejtësi dhe ku sfidat e sigurisë kombëtare zhvillohen çdo ditë, Shqipëria, si anëtare e NATO-s që nga viti 2009, është në një kërkim të vazhdueshëm për të zhvilluar dhe përsosur sistemin e saj arsimor ushtarak. Ky sistem nuk është thjesht një platformë për të mësuar teknikat dhe strategjitë e luftës, por një bazë për të ndërtuar dhe formuar udhëheqësit e ardhshëm ushtarakë që do të përballojnë sfidat e një mjedisi kombëtar dhe ndërkombëtar të ndërlikuar dhe të pandalshëm. Siç thotë rilindësi i madh shqiptar, Naim Frashëri: 'dhe drita e dijes, gjithmonë përpara do na shpjerë', kështu edhe ne kërkojmë që drita e dijes të udhëheqë ushtarakët tanë drejt një të ardhmeje më të sigurt dhe më të qëndrueshme.

Edukimi Ushtarak Profesional (EUP) në Shqipëri synon të përgatitë individë të aftë për të mbrojtur sovranitetin dhe integritetin kombëtar nëpërmjet një kuptimi të thellë të kërcënimeve tradicionale dhe jotradicionale. Përgatitja e ushtarakëve është një mision i ndërlikuar që kërkon një përshtatje ndaj një mjedisi strategjik që ndryshon vazhdimisht.

Ky shkrim do të trajtojë rolin e EUP si një kolonë e sigurisë kombëtare, duke ndërtuar një trupë ushtarake të përgatitur dhe të përkushtuar. Do të analizojë rolin e edukimit në përballjen e sfidave të sotme dhe të ardhshme dhe një përmirësim të vazhdueshëm të zhvillimeve në EUP, duke u bazuar në përvojat dhe praktikat më të mira të vendeve anëtare të NATO-s dhe vendeve të Baltikut.

Fjalët kyçe: Edukimi Ushtarak Profesional, NATO, mjedis strategjik, sistemi arsimor ushtarak, aftësi drejtuese, siguri kombëtare etj.

1. Rëndësia e edukimit ushtarak profesional: domosdoshmëri dhe nevojë për të ardhmen

Siguria kombëtare e Shqipërisë është një koncept i gjerë që përfshin shumë aspekte të ndryshme të mbrojtjes dhe mirëqenies të vendit. Një nga faktorët kyç për forcimin e kësaj sigurie është Edukimi Ushtarak Profesional, i cili është thelbësor për përgatitjen e individëve për rolet dhe përgjegjësitë ushtarake. EUP përfshin një gamë të gjerë përgatitjesh dhe zhvillimesh, që synojnë të përgatisin individët jo vetëm me njohuri teknike dhe taktike, por edhe me aftësi strategjike, mendimin kritik dhe aftësitë drejtuese (lidership).

Çfarë kuptojmë me EUP?

Në kushte të tilla, përgatitja e ushtarakëve, duhet të marrë një rëndësi të veçantë. Të mësuarit dhe dija janë dy koncepte, të cilat ndikojnë jo vetëm në përgatitjen e ushtarakëve por edhe në përmirësimin dhe zhvillimin e Forcave të Armatosura (FA). Siç theksonte ish-presidenti i SHBA, J.F. Kennedy, "Drejtimi dhe mësimi janë të pandashme nga njëri-tjetri." Ky parim është themelor për të kuptuar rëndësinë e EUP në përgatitjen e drejtuesve ushtarakë dhe në zhvillimin e FA-ve.

Dokumenti i miratuar nga NATO në vitin 2011, 'Generic Officer: Professional Military Education – Reference Curriculum', thekson se 'qëllimi themelor i arsimimit është të ngulitë dëshirën dhe aftësinë për të mësuar vazhdimisht. Sipas Eric Hoffer 'arsimimi nuk ka për qëllim vetëm të prodhojë njerëz të përgatitur, por të formojë individë që e duan të mësuarit dhe vazhdojnë të mësojnë në mënyrë të pavarur'.[1] Kjo qasje ndaj EUP thekson rëndësinë e zhvillimit të mendimit kritik dhe aftësive për zgjidhjen e problemeve, që janë thelbësore për personelin ushtarak dhe civil të FA-ve.

Roli i EUP-së në Sigurinë Kombëtare.

EUP ka një rëndësi strategjike dhe shërben si gur themeli në sigurinë kombëtare të Shqipërisë. Ky edukim pajis drejtuesit ushtarakë me cilësitë dhe aftësitë e nevojshme për të përballuar dhe kontrolluar sfidat e sigurisë në shekullin e 21-të. Nëpërmjet EUP-së, zhvillohet mendimi krijues dhe zgjerohen dijet, të cilat janë të rëndësishme për përshtatjen dhe ndryshimin e mjedisit të sigurisë.[2]

Cila është lidhja dhe ndërveprimi midis EUP dhe sigurisë kombëtare? Kjo është një pyetje shumë e rëndësishme e cila në radhë të parë kërkon të kuptojmë lidhje midis këtyre dy koncepteve dhe ndikimit të tyre në përgatitjen e personelit.

---

[1] NATO (2011) 'Generic Officer Professional Military Education: Reference Curriculum', p.4.

[2] Mie Augier and Wayne Hughes (2019) 'Innovative Thinking: The Role of Professional Military Education', https://cimsec.org/innovative-thinking-the-role-of-professional-military-education/, gjetur më 05 qershor 2024.

EUP është thelbësore për Sigurinë Kombëtare të Shqipërisë, pasi ofron bazën teorike dhe aftësitë praktike të nevojshme për zbatimin efektive të politikave të mbrojtjes kombëtare. Kurrikula e EUP-së shpesh përafrohet me dokumentet kryesore strategjike, duke siguruar që udhëheqësit ushtarakë janë përgatitur për të mbështetur dhe zbatuar strategjinë kombëtare.[3] Kjo lidhje siguron që të diplomuarit e EUP-së janë të aftë jo vetëm në njohjen e strategjive të mbrojtjes, por edhe në kontributin e tyre në zhvillimin e këtyre strategjive.

Përgatitja e udhëheqësve ushtarakë për mjedisin e ri të sigurisë.

Një sistem i zhvilluar i EUP-së luan një rol të rëndësishëm në ruajtjen e vlerave kombëtare dhe në përgatitjen e ushtarakëve për të mbrojtur interesat e vendit.[4] Nëpërmjet EUP-së ushtarakët fitojnë aftësitë për të përcaktuar prioritetet dhe interesat kombëtare dhe për të mbështetur parimet e sigurisë kombëtare Edukimi i vazhdueshëm dhe përshtatja me sfidat e reja ndihmojnë në sigurimin e një ushtrie të mirë trajnuar dhe të arsimuar, e cila është e gatshme të përballojë tensionet dhe konfliktet që mund lindin në rajon dhe më gjerë. Përveç kësaj, EUP luan rol të rëndësishëm në ruajtjen dhe vlerësimin e vlerave kombëtare. Ky sistem ngulit te personeli ushtarak ndjenjën e detyrës dhe përgjegjësisë në mbrojtjen e vlerave kombëtare dhe zhvillimin e vendit, e cila është e lidhur ngushtësisht me cilësinë e nivelit arsimor të bashkëkombësve tanë.

Sistemi i EUP i rekomanduar nga NATO.

Në vitin 2011, NATO prezantoi një propozim mbi zhvillimin dhe funksionimin e EUP-së, me qëllimin mbështetjen e vendeve të NATO-s dhe ato partnere në ndërtimin e një sistemi funksional për përgatitjen e ushtarakëve dhe civilëve. Në sistemin e rekomanduar nga NATO (shih tabelën nr.1)[5] paraqiten tre nivele të EUP-së. Ky propozim nuk prezanton dhe nuk rekomandon se si do të bëhet përgatitja e ushtarakëve dhe civilëve në nivelin e katërt (të fundit të EUP). Sistemi i EUP-së në Shqipëri dhe i vendeve të Baltikut e ka të përfshirë përgatitjen e nivelit të katërt. Mungesa e këtij niveli mund të krijojë së pari paqartësi në kuptimin dhe funksionimin e EUP- së dhe së dyti sa i vlefshëm do të jetë ky sistem për vendet e NATO-s dhe ato partnere.

Mungesa e koordinimit ose e përfshirjes së nivelit të katërt mund të paraqesë për shembull për FA të RSH, vështirësi në aplikimin e formulës së propozuar.

---

[3] S. Huffington, A Oler, and D Tretler (2021) ed 'A National Security Strategy Primer … The Assumptions pivotal to the National Security Strategy', National Defence University Press, Washington, D.C. p. 7.

[4] S. I Radda (2014) 'The Role of Education in Promoting National Security', Sociologica Department, Bayero University, Kano, Nigeria, pp …

[5] NATO, PfP Consortium and Canada., Generic Officer Professional Military Education: Reference Curriculum, NATO publication 2011, p. 5-6.

Mungesa e nivelit të katërt mund të krijojë probleme në ekuivalentimit e programeve mësimore dhe studentëve të cilët vijnë nga vende të tjera, për të studiuar në sistemin e EUP-së të Republikës së Shqipërisë. Në kapitullin pasardhës, lexuesi do të ketë mundësi të marrë dhe kuptojë më shumë mbi nivelet e EUP-së në FA të RSH.

Nivelet e edukimit	Funksionet	Grada
Kursi bazë i përgatitjes të oficerit	Të aftë për të drejtuar trupat në nivelin e togës	OF1/OF2 (Nëntoger/Toger)
Oficerët e rinj	Të aftë për të drejtuar trupat në nivelin e kompanisë	OF3/Major (i sapo graduar)
Niveli i mesëm/lartë	Të projektuar për të shërbyer shtabet e përgjithshme të komandimit për nivelet batalion, brigade etj.	OF3/OF4 (Major (me eksperiencë)/Nënkolonel)

Tabela nr. 1: Sistemi i EUP i rekomanduar nga NATO

Sistemi i EUP në Kolegjin e Vendeve të Baltikut.

Kolegji i Vendeve të Baltikut është krijuar në vitin 1999, si element i rëndësishëm në rritjen dhe përsosjen e përgatitjes së oficerëve dhe civilëve nga vendet krijuese si: Estonia, Letonia dhe Lituania. Ish-presidenti i Estonisë z. Lennart Mery në ceremoninë e hapjes së kolegjit do të theksonte tre detyra kryesore për t'u ndjekur në përgatitjen e studentëve:

1) Ndërtimi i një bashkëpunimi sa më të ngushtë midis tre vendeve të Baltikut në përballimin e sfidave të sigurisë.

2) Forcimi dhe përgatitja sa më mirë e strukturave të forcave të armatosura.

3) Angazhimi me fqinjët në krijimin e paqes në rajon.[6]

Që nga ajo kohë Kolegji ka një mision shumë të rëndësishëm në përgatitjen e udhëheqësve të së ardhmes më cilësitë e nevojshme dhe aftësitë krijuese në kuptimin sa më mirë të sfidave të sigurisë. Kurrikula është e hartuar për të përballuar sfidat e ndërlikuara në rajonin e detit të Baltikut me vëmendje të veçantë mbi Federatën Ruse, rolin dhe interesat e NATO-s dhe BE-së.[7] EUP në vendet e Baltikut përfshin një numër kursesh dhe programesh të përgatitjes dhe arsimimit të oficerëve të rinj dhe të oficerëve të niveleve të larta. Në sistemin e EUP-së, ka katër nivele të përgatitjes dhe zhvillimit. Niveli i parë dhe i dytë ofrojnë përgatitjen bazë dhe arsimimin e oficerëve të rinj. Këto nivele përgatitjeje janë përgjegjësi e vendeve të Baltikut.

---

[6] Corum J., Johanson A., (Quoted here) 20th Years of the Baltic Defence College: Professional Military Education in the Baltic States, Valipress OU Estonia, 2019, pp. 5.

[7] BALTDEFCOL, HCSC 2024 Course Plan (Plani i Kursit), Tartu, Estonia, fq. 5-6 & 20

Ndërsa kolegji është përgjegjës për nivelin e tretë (kursin e Komandave dhe Shtabeve të Bashkuara) dhe nivelin e katërt kursin e lartë (të studimeve të komandimit). Kjo përqasje në lidhje me përgatitjen dhe zhvillimin e oficerëve paraqitet në tabelën nr. 2.[8]

Niveli i Parë	Niveli i Dytë	Niveli i Tretë	Niveli i Katërt
Niveli Bazë	Oficeri i Ri	I avancuar	Niveli i Lartë
Niveli Taktik	Niveli Taktik	Niveli Operacional	Niveli Strategjik
Niveli bazë dhe kurset për specialitet	Kursi i Kapitenit dhe Kursi i nivelit të mesëm	Kursi i Komandave dhe Shtabeve të Bashkuara	Kursi i Lartë i Studimeve të Komandimit
Akademia kombëtare ose ndërkombëtare	Akademia kombëtare ose ndërkombëtare	Kolegji i Vendeve të Baltikut ose Kolegje ndërkombëtare ose të luftës	Kolegji i Vendeve të Baltikut ose Kolegje ndërkombëtare ose të luftës
OF 1 (Nëntoger)	OF 1 – OF 2 (Nëntoger-Toger)	OF 3 – OF 4 (Major-Nënkolonel) dhe civil	OF 4 – OF 5 (Nënkolonel-Kolonel) dhe civil

Tabela nr. 2 Sistemi i EUP-së të Vendeve të Baltikut

2. Vështrimi historik dhe vizioni i EUP në FA

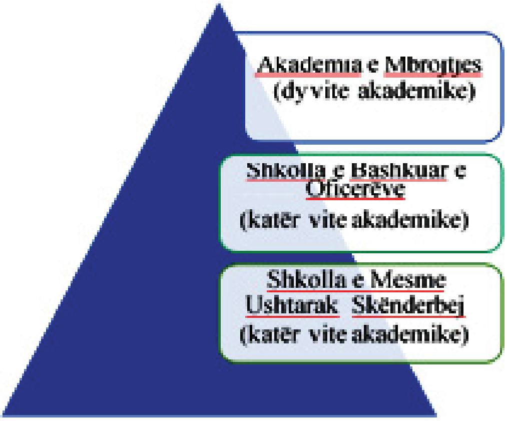
EUP-ja në Shqipëri ka një histori të gjatë dhe komplekse, duke luajtur një rol thelbësor në përgatitjen e trupave ushtarake për sfidat e sigurisë. Historia fillon nga periudha e shtetit të Arbrit, ku familjet fisnike si Ballshajt, Muzakajt, Dukagjinasit dhe Kastriotët mbanin forca të armatosura të trajnuara dhe të paguara individualisht për të përballuar situatat luftarake. Në raste të veçanta, këto familje kontribuonin për ushtrinë e shtetit të Arbrit. Më konkretisht, origjina e zhvillimit të edukimit ushtarak fillon në vitet 1797-1822, ku pashallëku i Janinës, me në krye Ali Pashë Tepelenën, në Bonilë, krijojë shkollën e parë të artilerisë, xhenios dhe kalorësisë, me pjesëmarrjen e instruktorëve francezë, italianë dhe shqiptarë. Në fund të shekullit XIX, Shqipëria u përball me sfida të mëdha nga Perandoria Osmane dhe ambiciet e Perandorisë Ruse. Në këtë periudhë, u krijua Lidhja e Prizrenit (1878), e cila synonte mbrojtjen e territoreve shqiptare dhe krijimin e një shteti të pavarur. Lidhja organizoi dhe mobilizoi forcat ushtarake, megjithëse përballoi vështirësi të mëdha.

Pas shpalljes së pavarësisë në 1912, ushtarakët shqiptarë ishin kryesisht të përgatitur në shkollat osmane. Gjatë Luftës së Parë Botërore (1913-1919), vende si Austro-Hungaria, Italia dhe Franca kontribuuan në përgatitjen e ushtarakëve shqiptarë. Në 1919, qeveria e përkohshme hapi një shkollë për përgatitjen e oficerëve dhe xhandarëve.

---

[8] HCSC (Higher Command Studies Course/Kursi i Lartë i Studimeve të Komandimit), zhvillimi i kurrikulës, (2024), Tartu, Estoni, fq. 6.

Institucionalisht shkolla e parë ushtarake u krijuar më 26 tetor 1926. Nga 1920 deri në 1939, në Shqipëri funksionuan shkolla që ofronin kurse gjashtëmujore për përgatitjen e oficerëve. Mbretëria Shqiptare e asaj kohe krijoj shkollën për përgatitjen e ushtarakëve në vitin 1928. Ndërsa, gjatë Luftës së Dytë Botërore, Ushtria Nacionalçlirimtare (UNÇL) përgatiti kuadrot e saj në kushte të vështira, sipas nevojave luftarake. Pas çlirimit të Shqipërisë më 29 nëntor 1944, autoritete vendore të asaj kohe, vendosën të krijonin bazat e edukimi ushtarak, duke krijuar më 8 nëntor 1944 Shkollën e Bashkuar të Oficerëve, që më vonë mori emrin “Enver Hoxha”. Kjo shkollë përgatiste oficerët për armët e këmbësorisë, artilerisë dhe prapavijës. Gjithashtu, në Vlorë u hapën shkollat për përgatitjen e oficerëve të detarisë dhe aviacionit. Ndërsa Shkolla e Mesme Ushtarake Skënderbej u krijua më 28 mars 1945, për përgatitjen e partizanëve të rinj. Vendimi përfundimtar u mor më 10 maj 1958, duke krijuar bazën ligjore për krijimin e Shkollës së Lartë Ushtarake. Më vonë më 15 shtator 1961, me vendim të qeverisë u emërtua Akademia Ushtarake. Akademia Ushtarake ose e Mbrojtjes, ka ofruar kualifikime të avancuara dhe strategjike për oficerët nga vitin 1958 deri në ditët e sotme. Por cila ishte në të vërtetë sistem EUP para viteve 90, në Shqipëri. (Shih figurën)



3. Edukimi Ushtarak Profesional në Republikën e Shqipërisë, pas vitit 1992

Le ta fillojmë me pyetjen: Cili është misioni i Edukimit Profesional në Shqipëri? EUP në Shqipëri synon të formojë një trupë drejtuesish të aftë, oficerë dhe nënoficerë, të përgatitur për të kryer me sukses detyrat e ngarkuara dhe për t’i shërbyer kombit. Këta drejtues duhet të pajisen me aftësi për të menduar dhe analizuar në mënyrë kritike dhe krijuese për drejtimin e FA-ve, ndërveprimin me aleatët në NATO dhe ballafaqimin me rreziqet e krijuara nga kundërshtarët e mundshëm. Përgatitja ushtarake e personelit dhe devotshmëria ndaj atdheut dhe kombit janë objektivat kryesorë të misionit dhe qëllimeve të EUP.

Edukimi ushtarak profesional në Shqipëri është pjesë integrale e sistemit të arsimimit kombëtar. Institucionet kryesore që merren me arsimimin e ushtarakëve (oficerëve dhe nënoficerëve) dhe civilëve janë Akademia e Forcave të Armatosura (AFA) dhe Kolegji i Mbrojtjes dhe Sigurisë (KMS). Këto institucione synojnë arsimimin dhe përgatitjen e ushtarakëve dhe civilëve në të gjitha nivelet e drejtimit të FA-ve dhe institucioneve të tjera vendore që trajtojnë çështjet e sigurisë dhe mbrojtjes. Misioni i arsimimit ushtarak është thelbësor për të kuptuar natyrën dhe aftësitë përgatitëse të këtyre institucioneve.[9]

Objektivat e përgatitjes.

Sipas statusit të Akademisë të Forcave të Armatosura të miratuar në vitin 2017, janë përcaktuar objektivat dhe detyrat për zhvillimin dhe mbarëvajtjen e arsimit ushtarak në Republikën e Shqipërisë. Akademitë kanë për detyrë të përgatisin dhe edukojnë personelin ushtarak dhe civil në të gjitha nivelet e FA-ve. Këtu përfshihet edukimi i ushtarakëve në nivelin e parë, të dytë, të tretë dhe të katërt. AFA-ja ofron edukimin në Bachelor, Master (në Arte ose në Shkenca) dhe studimet në doktoratë. Kolegji i Mbrojtjes dhe Sigurisë përgatit oficerë nga grada e Kapitenit deri në gradën e Kolonelit, duke kaluar nga niveli i dytë deri tek i katërti i EUP-së.

Rëndësia e Kurrikulës në Edukimin Ushtarak.

Përgatitja e kurrikulave luan një rol thelbësor në mbarëvajtjen e procesit mësimor dhe në arritjen e objektivave edukative të trupës studentore ushtarake. Kurrikula ndikon në mënyrë të konsiderueshme në aspekte të ndryshme të filozofisë, psikologjisë dhe sociologjisë, duke qenë një element thelbësor, kompleks dhe i rëndësishëm për pedagogjinë. Qëllimi kryesor i kurrikulës është zhvillimi i procesit mësimor dhe përgatitja e studentëve ushtarakë për të përmbushur objektivat e tyre mësimore. AFA dhe KMS duhet të përqendrohen në përmirësimin dhe përditësimin e kurrikulës, me synim përshtatjen ndaj rreziqeve bashkëkohore dhe kuptimin e mjedisit të sigurisë, i cili po bëhet gjithnjë e më i paparashikueshëm. Për ta arritur këtë, kurrikula duhet të rishikohet çdo vit dhe të ndryshohet sipas një përqindjeje të përcaktuar me ligj ose rregullore të brendshme (SOP)[10] të institucioneve arsimore ushtarake. Kjo kërkon mbështetje të fuqishme nga institucionet eprore, si Ministria e Mbrojtjes (MM) dhe Shtabi i Përgjithshëm i Forcave të Armatosura (SHPFA), në mënyrë morale, financiare dhe materiale, për të siguruar një sistem arsimor të shëndetshëm dhe të qëndrueshëm.

Iniciativa e Qeverisë së Shqipërisë për përmirësimin e EUP.

Në vitin 2021, Qeveria e Shqipërisë dhe Ministria e Mbrojtjes deklaruan se do t'i kushtojnë më shumë vëmendje përgatitjes dhe arsimimit në fushën e mbrojtjes. Kjo iniciativë synon shfrytëzimin e dy burimeve kryesore: (1) përvojën brenda Forcave të Armatosura dhe (2) përvojën e vendeve më të zhvilluara anëtare të NATO-s. Shqipëria ka dërguar dhe përgatitur një numër të madh ushtarakësh në akademitë ushtarake më të njohura të SHBA, Mbretërisë së Bashkuar, Gjermanisë, Italisë, Turqisë, Greqisë dhe vendeve të tjera, duke përfituar nga përvoja dhe marrëdhëniet e krijuara me institucionet simotra. Këto përvoja dhe marrëdhënie do të kontribuojnë në reformimin dhe përmirësimin e sistemit të arsimimit ushtarak në Shqipëri.

---

[9] Statusi i AFA-së, miratuar në vitin 2017.

[10] SOP – Standard Operating Procedure (*Standarde të Procedurave Operative/Operacionale*).

Panorama e Edukimit Ushtarak Profesional.

Arsimimi Ushtarak Profesional përgatit oficerët në 4 nivele ose fusha kryesore:

Niveli i parë - Përqendrohet në përgatitjen e oficerëve të rinj, përgjegjësi e Akademisë të Forcave të Armatosura. Në të shkuarën, ky nivel ishte i lidhur me Akademinë Ushtarake 'Skënderbej'.

Niveli i dytë, i tretë dhe i katërt - Të gjitha nivelet e tjera duhet të jenë përgjegjësi e Kolegjit të Mbrojtjes dhe Sigurisë. Këto nivele përfshijnë përgatitjen taktike, operacionale dhe strategjike të oficerëve (Shih tabelën 3).

Edukimi Ushtarak Profesional në Forcat e Armatosura të RSH

Niveli i parë	**Niveli i dytë**	**Niveli i tretë**	**Niveli i katërt**
Përgatitja bazë (*Programi Bachelor - 3 vjet*) kadet / student	Përgatitja e oficerëve të rinj	Niveli i avancuar	Niveli i lartë
Niveli Taktik	**Niveli Taktik**	**Niveli Operacional**	**Niveli Strategjik**
Kurse të tjera të përgatitjes të oficerit të ri (*kontingjente nga UT – 9 muaj kurs*)	Kursi Themelor i Oficerit të Shtabit **(KTHOSH)**	Kursi i Komandës dhe i Shtabit të Përgjithshëm **(KKSHP).** Kursi i Lartë i Oficerit **(KLO)**	Kursi i Lartë për Sigurinë dhe Mbrojtjen **(KLSM)**
Institucioni përgjegjës: Akademia e Forcave të Armatosura	**Institucioni përgjegjës**: Kolegji i Mbrojtjes dhe Sigurisë	**Institucioni përgjegjës**: Kolegji i Mbrojtjes dhe Sigurisë	**Institucioni përgjegjës**: Kolegji i Mbrojtjes dhe Sigurisë

Grada: Nëntoger -Toger (OF1)	**Grada**: Kapiten (OF-2)	**Grada**: Major-N.kolonel (OF3 - OF4&Civil)	**Grada**: N.kolonel - Kolonel (OF4 – OF5 & Civil)
(*Programet Master (MA & MSc) & Doktorata (PhD)*) **Institucioni përgjegjës**: Akademia e Forcave të Armatosura			

Tabela nr. 4. Akademia e Forcave të Armatosura/Kolegji i Mbrojtjes dhe Sigurisë

4. Sfidat dhe perspektivat për të ardhmen

AFA merret me përgatitjen e studentëve/kadetëve ushtarakë, ndërsa KMS zhvillon disa kurse, si Kursin Themelor të Oficerit të Shtabit (KTHOSH), Kursin e Komandës dhe Shtabit të Përgjithshëm (KKSHP), Kursin e Lartë të Oficerit (KLO) dhe Kursin e Lartë për Sigurinë dhe Mbrojtjen (KLSM). Këto kurse janë krijuar për të përgatitur ushtarakët me grada OF2/OF3/OF4 dhe OF5. Ndërsa mjedisi i sigurisë dhe arti ushtarak ndryshojnë, kurrikula duhet të përshtatet në lidhje me ndryshimet. Në këtë kontekst, lindin disa pyetje kyçe të cilat kërkojnë përgjigje:

- Çfarë duhet përmirësuar në AFA dhe KMS?
- Si duhet ndërtuar sistemi arsimor?
- Cilat do të jenë burimet financiare dhe njerëzore?

Për të përmirësuar AFA-në dhe KMS-së, disa masa janë të nevojshme:

- Zhvillimi i strukturës: Struktura aktuale duhet të vazhdojë të zhvillohet jo të ndryshojë (*evolution not revolution*). Është e nevojshme që stafi akademik të vlerësohet dhe të rifreskohet.

- Pasurimi i kurrikulës dhe literaturës: Literatura (si në formë të shtypur ashtu edhe online) duhet të pasurohet për të pasqyruar zhvillimet më të fundit në fushën ushtarake dhe atë të sigurisë.

- Rishikimi i nivelit të tretë të edukimit ushtarak: Niveli i tretë i arsimimit duhet të rishikohet në përputhje me praktikat e vendeve anëtare të NATO-s. Ligji që rregullon sistemin arsimor në fushën e mbrojtjes mund të ketë nevojë për ndryshime për të reflektuar këto zhvillime dhe përparimet teknologjike.

Ndryshimet e nevojshme në kurset e KMS.

Kursi i Komandës dhe Shtabit të Përgjithshëm (KKSHP) dhe Kursi i Lartë i Oficerit (KLO) përbëjnë nivelin e tretë të edukimit në fushën e mbrojtjes. Këtu ekziston nevoja për ndryshim dhe përmirësim. Përvojat më të mira të vendeve perëndimore dhe Kolegjit të Baltikut ofrojnë modele që mund të përshtaten me mjedisin shqiptar. Për shembull, KMS mund të integrojë KKSHP dhe KLO në një kurs të përbashkët të emërtuar Kursi i Komandave të Bashkuara dhe Shtabit të Përgjithshëm (KKBSHP).

Ky kurs i integruar do të kursejë kohë dhe burime financiare dhe do të përshtatë kurrikulën për të reflektuar ndryshimet në natyrën e luftës dhe të mjedisit të sigurisë. Kursi i ri do të zgjasë jo më shumë se 10-11 muaj. Ndërsa disa pjesë të programit të KKSHP mund të transferohen në Kursin Themelor të Oficerit të Shtabit (KTHOSH), duke e zgjatur këtë kurs nga 4 në 5-6 muaj, në përputhje me standardet e vendeve të Baltikut. Ndërsa, Kursi i Lartë për Sigurinë dhe Mbrojtjen (KLSM) duhet të zgjasë rreth 5 muaj ose 23 javë, duke përfshirë një gamë të gjerë temash në fushën e sigurisë dhe mbrojtjes, si mjedisi ndërkombëtar i sigurisë, NATO/Rusia, politika e mbrojtjes, planifikimi/planëzimi i mbrojtjes (strategjik) dhe menaxhimi, parandalimi i rreziqeve, etj. Kjo do të përfshijë më shumë aktorë nga brenda dhe jashtë vendit.

Stafi Akademik dhe puna kërkimore në AFA dhe KMS.

AFA dhe KMS duhet të kenë një trupë akademike të përgatitur me standardet më të mira brenda dhe jashtë vendit. Njohja e gjuhës angleze është thelbësore për të përthithur informacionin dhe dijen e nevojshme. Institucioni duhet të konsiderohet si shtylla kurrizore e FA-ve. Pa të, nuk ka zhvillim të qëndrueshëm dhe siguri kombëtare.

Për të rritur cilësinë e edukimit, është thelbësore të përmirësohet vlerësimi i stafit akademik. Ata që shërbejnë në AFA dhe KMS, duhet të jenë ndër më të mirët dhe të kenë një avantazh ndaj të tjerëve në sistem. Pa trupë akademike cilësore nuk ka ushtarakë të përgatitur. *Arsimimi*, thotë Nelson Mandela, është arma më e fuqishme, me të cilën ju mund të ndryshoni botën. Botën e brendshme të FA-ve dhe pjesëtarëve të saj. *Qëllimi i edukimit profesional ushtarak,* siç thotë Louis Simpson, *nuk duhet të jetë vetëm përgatitja e burrave për luftë, por për një kohë më të gjatë*.

AFA dhe KMS duhet të ketë një sistem të brendshëm komunikimi (*intranet/computer network*) për të lehtësuar komunikimin me stafin akademik dhe studentët. Për shembull, në Kolegjin e Baltikut përdoret ILIAS (*software*) për komunikimin e brendshëm. Po ashtu, faqja zyrtare e internetit e AFA-së dhe KMS-së, duhet të vetë-menaxhohet dhe të ofrojë informacionin e nevojshëm për publikun dhe komunitetin akademik.

Institucionet e edukimit ushtarak duhet të jenë model jo vetëm në fushën e arsimimit, por edhe të vlerave që ajo mbart. Sot na duhen ushtarakë me njohuri jo vetëm në fushën e mbrojtjes dhe të sigurisë, por edhe në politikë apo në fushën e ekonomisë. Për ta ilustruar, dua të sjell një thënie te kolonel Lincoln në një letër drejtuar ish-përgatitësit të tij në West Point: '*Unë kam filluar të mendoj se ne na duhet një model i oficerit të shtabit, i cili të ketë tre koka – një për politikë, një për ekonomi dhe një për çështjet ushtarake*.'[11]

Përfundime

Ndërtimi dhe përmirësimi i mbarëvajtjes në institucionet akademike në fushën e mbrojtjes kërkojnë vullnet, mbështetje dhe transparencë. Akademitë ushtarake janë përgjegjëse për përgatitjen e ushtarakëve me dijet dhe njohuritë e nevojshme në të gjitha nivelet e EUP. Zbatimi i politikave arsimore dhe kurrikulës akademike kërkon dy gjëra kryesore: infrastrukturën e duhur dhe stafin akademik të arsimuar. Arritja e këtyre objektivave kërkon investim dhe vëmendje ndaj personelit (*invest in people*). Akademitë ushtarake duhet të përgatisin mendje krijuese që do të drejtojnë njësitë dhe formacionet luftarake sipas standardeve të NATO-s.

EUP duhet të krijojë dhe mundësojë kurrikulë të përditësuar, sipas kërkesave dhe standardeve të diktuara nga zhvillimet teknologjike dhe mjedisi i sigurisë. Kurrikula e rishikuar dhe e përmirësuar duhet të krijojë mjedis akademik tërheqës dhe cilësor për përvetësimin e dijeve dhe metodave të reja të luftimit dhe përballimit të rreziqeve. Në një mjedis sigurie gjithnjë e më të paparashikueshëm, akademitë ushtarake janë vendet ku mund të përvetësohen dhe debatohen rreziqet dhe sfidat e shekullit të 21-të. Lufta kibernetike dhe informacioni i rremë po dominojnë mjedisin e sigurisë dhe sigurinë kombëtare dhe ne duhet të jemi të përgatitur për këto sfida. Kjo realizohet përmes institucioneve të standardizuara dhe trupës mësimdhënëse të përgatitura.

Ushtarakët e përgatitur dhe mendimi kritik do ta lehtësojnë kuptimin e mjedisit të sigurisë dhe përballimin e rreziqeve. EUP gjithmonë do të ndikohet nga sfidat dhe mundësitë e reja. Ne duhet të kuptojmë se çfarë duam të mësojmë në Akademi, kush duhet të vijë në AFA dhe KMS dhe kush duhet t'i përgatisë? Objektivi i reformimit duhet të jetë përmirësimi i mjedisit akademik dhe ndryshimet duhet të jenë efektive dhe të nevojshme. Ndërsa ne mund të ndryshojmë ose ristrukturojmë institucione të arsimimit ushtarak, përgatitja e trupës akademike mbetet thelbësore. Pa një trupë të përgatitur mësimdhënëse, çdo përpjekje është e destinuar të dështojë. Pedagogët dhe instruktorët janë

---

[11] Fred Kaplan (2014) '*The Insurgents: David Petraeus and the Plot to Change the American Way of War*', Simon & Schuster Paperbacks, New York, pp.6.

‘*thembra e Akilit*’ në reformimin dhe mbarëvajtjen e institucioneve të arsimimit ushtarak.

Ky shkrim nuk pretendon të japë përgjigje ose zgjidhje për modelin ose sistemin më të mirë të përgatitjes në fushën e EUP-së në Forcat e Armatosura të Republikës së Shqipërisë. Stafet akademike, hartuesit e kurrikulave dhe njohësit e arsimimit ushtarak mund të japin përgjigje më të sakta. Të gjithë duhet të biem dakord që akademitë dhe kolegjet ushtarake duhet të marrë vendin që u takon. AFA dhe KMS do të jenë gur themeli në formësimin dhe përgatitjen e ushtarakëve me dijet dhe njohuritë e nevojshme për mbrojtjen e vendit dhe përballimin e rreziqeve. Ne duhet të ndërtojmë sisteme që do t'i rezistojnë kohës.

Bibliografia

1. Mie Augier and Wayne Hughes (2019) *Innovative Thinking: The Role of Professional Military Education*, https://cimsec.org/innovative-thinking-the-role-of-professional-military-education/, gjetur më 05 qershor 2024.
2. S. Huffington, A Oler, and D Tretler ed. *A National Security Strategy Primer ... The Assumptions pivotal to the National Security Strategy*, National Defence University Press, Washington, D.C. (2021).
3. S. I Radda, *The Role of Education in Promoting National Security*, Sociologica Department, Bayero University, Kano, Nigeria, (2014).
4. NATO, PfP Consortium and Canada., Generic Officer Professional Military Education: Reference Curriculum, NATO publication 2011.
5. Corum J., Johanson A., *20th Years of the Baltic Defence College: Professional Military Education in the Baltic States*, Valipress OU Estonia, 2019.
6. HCSC (Higher Command Studies Course/Kursi i Lartë i Studimeve të Komandimit), zhvillimi i kurrikulës, (2024), Tartu, Estoni.
7. Sabri Godo, *Ali Pasha*, Tirana, 1989.
8. Fred Kaplan ‘*The Insurgents: David Petraeus and the Plot to Change the American Way of War*’, Simon & Schuster Paperbacks, New York, (2014).
9. Rupert Smith ‘*The Utility of Force: The Art of War in the Modern World*’, Penguin, London, (2009).

Krijimtaria dhe suksesi

Prof. Asoc. Dr. Edmond BRANESHI
Shef Grupi në Shkenca Komunikimi, FMS

Trajtesë e shkurtuar.

Deri para disa vitesh, dija ishte ajo që e bënte një organizatë të ishte "njëshi" në fushën e saj. Njohuritë, kërkimet, trajnimet dhe përvoja ishin karakteristikat që u jepnin organizatave përparësi ndaj konkurrentëve. Por tani, kohët dhe mjedisi kanë ndryshuar. Sigurisht, që informacioni dhe njohuritë janë akoma pika kyçe për çdo organizatë në fushat përkatëse, por ato nuk janë të mjaftueshme për të garantuar mbijetesën dhe qenien në krye. Për këtë arsye, duhet të jemi në gjendje të përshtatemi dhe evoluojmë, duke iu përgjigjur ndryshimeve të vazhdueshme dhe të papritura që lindin, si brenda organizatës ashtu edhe në drejtim. Suksesi ynë varet nga ajo që ne jemi në gjendje të krijojmë. Prandaj krijimtaria merr një rëndësi të madhe për ecurinë dhe suksesin e organizatës. Ne duhet të vetë ndërgjegjësohemi se krijimtaria ekziston brenda nesh, thjesht duhet të mësojmë ta bëjmë atë të rishfaqet.

Çdo punonjës (vartës) në organizatë duhet të sjellë, të eksplorojë dhe të zhvillojë ide të reja, për të cilat do t'i njihet merita. Paaftësia për të sjellë ide të reja nënkupton paaftësi për ta bërë siç duhet punën. Fatkeqësisht, një numër jo i vogël njerëzish bëjnë shumë pak, për të mos thënë aspak, në lidhje me mendimin krijues. Ata kanë mbetur brenda zonës së rehatisë, duke u përpjekur t'i ruajnë të pandryshuara ato rezultate që kanë arritur në të kaluarën. Këta njerëz janë duke humbur një nga mundësitë më të mëdha për të ecur drejt përparimit dhe suksesit.

Drejtuesit duhet të besojnë se risitë duhet të jenë të vijueshme në organizatën që drejtojnë dhe duhet të përkrahen pa rezerva. Në këtë kuadër, drejtuesit *duhet të krijojnë mjedis të këndshëm, ku krijimtaria të jetë pjesë e mendësisë së punës së kujtdo, kudo në çdo çast. Ajo duhet të bëhet pjesë e ADN-së së strukturave dhe tipar dallues i çdo punonjësi në organizatë. Edhe synimi i këtij shkrimi është që të japë konceptin bazë mbi krijimtarinë, rëndësinë që ka ajo në suksesin e organizatës, karakteristikat e njerëzve krijues, si dhe roli i drejtuesit për të pasur një mjedis krijues të përhershëm në organizatë, me qëllim që "ëndrrat e projektuara" të bëhen realitet. Krijimtaria luan një rol jetësor në kohën e sotme dhe ne duhet të mësojmë të kemi një qasje krijuese për zgjidhjen e problemeve dhe sfidave që do të hasim.*

Fjalë kyçe: krijimtari, proces krijues, veprimtari krijuese, rëndësia e krijimtarisë, njerëz krijues, karakteristikë, risi, drejtues, organizatë, sfidë.

Hyrje

Zhvillimi i vrullshëm dhe sfidat e njëpasnjëshme që përçon mjedisi bëjnë që shumë faktorë, të cilët më parë përbënin përparësi për organizatat, sot të mos jenë më të tillë. Kjo ndodh si për aftësitë, ashtu edhe për informacionin apo teknologjinë. Ne nuk mund të mbetemi me shpresën se organizatat e tjera, që janë konkurrentet tanë nuk do të jenë po aq të zot sa ne, sepse edhe sikur të duam, nuk mund ta ndalim dot përmirësimin dhe ecurinë e tyre. Sot kushdo mund ta gjejë informacionin apo teknologjinë që i nevojitet, mjafton që të investojë për to. Nëse ndërgjegjësohemi se sot, pothuajse çdo gjë është e arritshme nga të gjithë, ajo që ngelet unike dhe që do të bëjë ndryshimin, është aftësia për të krijuar vlerë edhe në këto kushte. Pikërisht kjo është krijimtaria, e cila nuk është një talent hyjnor të cilin e zotërojnë vetëm pak njerëz. Ajo është një shprehi të cilën të gjithë ne mund dhe duhet ta zhvillojmë. Për këtë arsye, krijimtaria është një mjeshtri, e cila njëlloj si ngarja e biçikletës, ose si puna me një kompjuter mund të mësohet dhe të zhvillohet, duke u praktikuar. Një ide ose një perceptim i ri, mund të jetë i mjaftueshëm për ta ndryshuar rrjedhën e drejtimit të një karriere, ose të një organizate të tërë.

Ne duhet të sfidojmë konceptet dhe perceptimet e pranuara nga të gjithë jo sepse ato janë të gabuara apo të papërshtatshme, por sepse kështu mund të gjejmë dhe më pas të zhvillojmë një alternativë më të mirë. Këtë mënyrë të menduari duhet ta përqafojmë në organizatën që drejtojmë dhe të gjithë drejtuesit vartës duhet që ta nxisin, pavarësisht pozicionit në nivelin e hierarkisë. Vetëm në këtë mënyrë, krijimtaria do të konsiderohet si një pritshmëri prej të gjithëve dhe si një proces shumë i rëndësishëm për të qenë vazhdimisht të renditur në krye.

1. Koncepti mbi krijimtarinë

Origjina e fjalës "*krijimtari*" vjen nga latinishtja "*creare*" që do të thotë "*të krijosh nga asgjëja*". Thelbi i krijimtarisë është krijimi i diçkaje të re, që nuk ka ekzistuar më parë. Me krijimtari nënkuptojmë aftësinë e njeriut për të qenë krijues, inteligjent, me një imagjinatë të aftë që e ndihmon të ketë një jetë dhe veprimtari më tërheqëse dhe interesante[1]. Krijimtaria është aftësia për të sjellë diçka të re në jetë. Ajo paraqitet në mendimet dhe veprimet e njerëzve. Prodhimet krijuese lindin nëpërmjet procesit të krijimtarisë që ndodh tek një person ose grup personash. Këto prodhime mund të jenë shumë të ndryshme si për shembull, të paprekshme (një ide, një teori shkencore, një kompozim muzikor, formimi i një sistemi të ri filozofik etj.,) ose një objekt fizik (një shpikje, një projekt i ri, një vepër letrare apo arti, etj.). Prodhimet krijuese dallohen nga njëri-tjetri nga origjinaliteti, zgjedhja, vlerat, përdorimi etj.

Te njerëzit krijues, pavarësisht moshës së tyre, prejardhjes etnike, kombësisë etj., ne gjejmë trajta të caktuara përsëritëse: aftësi për të menduar në mënyrë metaforike, analogjike, logjike, pavarësinë e gjykimit, kundërshti të thjeshtësisë etj. Krijimtaria është një ndër kualifikimet më kyçe për drejtuesit, pasi roli që luan FA në një shoqëri demokratike është mjaft i rëndësishëm. Koncepti i "krijimtarisë" është një koncept shumë i gjerë, vetë termi "krijimtari" është një ndër termat më të përdorur në mënyrë të veçantë, në dy dekadat e para të këtij shekulli, dhe i tillë ka për të mbetur edhe në të ardhmen, pasi zhvillimi i shoqërisë është një proces gjithnjë i vazhdueshëm.

Psikologë, psikoanalistë etj., shpeshherë e paraqesin krijimtarinë si pjesën më të qëndrueshme të personalitetit të njeriut. Studiues të shumtë (Rohrbach, Köstler, Taylor, Frojd, Geyer etj.) japin përkufizime të ndryshme për krijimtarinë, por thelbi i çështjes qëndron në sintezën e pikëpamjeve të tyre. Ajo që bie në sy është se krijimtaria cilësohet aftësia për të gjeneruar ide të reja dhe për të njohur perspektiva të reja dhe të dallueshme për një problem ose mundësi. E përbashkëta e tyre është se veprimtaria krijuese kurrë nuk lind nga "hiçi, pra nga "asgjëja", përkundrazi, sekreti i krijimtarisë qëndron në atë që, dy modele të menduari deri tani të para si të shkëputura (logjika) lidhen me një ide të re (fantazia), nëpërmjet përfytyrimit të dyfishtë[2].

Krijimtaria kërkon thyerje të rutinës, të mendosh jashtë kornizave, të jesh mendjehapur. Njerëzit që janë kuriozë për të zbuluar, të hapur ndaj eksperimenteve, entuziastë nga natyra, optimistë për arritjet, që nuk dekurajohen nga dështimet janë më të prirur për të qenë krijues. Kur përpiqeni të bëni inovacion, asnjëherë nuk mund të jeni 100% të sigurtë që do të funksionojë. Mos u trembni nga dështimi. Dështimi ju mëson të paktën çfarë të mos bëni.

---

[1] Vasil Naçi, Alma Bici, "Roli i marketingut dhe Kreativiteti", botuar nga Agna Leadership Academy, Viti 2012, faqe 89.

[2] Q. Orhani, E. Braneshi, M. Cukalla, "Udhëheqja Ushtarake 2", shtypur në Shtypshkronjën "Grand Prind", Tiranë 2011, faqe 159.

Thomas Edison-i, shpikësi i madh i kohërave moderne u bind se eksperimentimi ishte thjesht një proces eliminimi. Si pasojë, ai mbante të dhëna të sakta për çdo eksperiment. Sapo ai kishte vendosur se një shpikje ishte e mundur, ai i përkushtohej procesit të eliminimit të rrugëve që nuk do të funksiononin derisa metoda e vetme e mbetur të ishte e vetmja që do të funksiononte. Njerëzit duhet të bëjnë të njëjtën gjë. Në çdo kohë që ata përpiqen dhe dështojnë, duhet ta konsiderojnë atë si një përvojë të nxëni e cila i çon një hap më pranë suksesit. Ashtu siç thekson edhe Henry Ford: "*Dështimi është thjesht një mundësi për të nisur sërish* më zgjuarsisht".[3] Pra, provoni mënyra të reja që mund të funksionojnë më mirë.

Të gjithë kanë aftësinë për të menduar në mënyrë krijuese, si dhe aftësinë për të përdorur më shumë pjesën e trurit që mendon siç duhet. Thjesht të qenit i vetëdijshëm për nevojën për të qenë më krijues në punë mund t'ju ndihmojë të kini një paraqitje më të mirë në punën tuaj brenda organizatës.

Organizatat sot kanë nevojë për krijimtari dhe ato duhet ta ushqejnë atë. Krijimtaria kërkon kurajë, kërkon të besojmë se gjithkush mund të jetë krijues, kërkon fokus te zgjidhjet, mendim pozitiv, rritjen dhe shkëmbimin e njohurive dhe zhvillimin e kurajës për të qenë ndryshe. Krijimtaria kërkon që të jemi të hapur, të zgjerojmë imagjinatën, të shikojmë dështimin si mundësi për të mësuar, të zgjedhim miq krijues, të gjejmë kohë për të praktikuar krijimtarinë dhe të kujdesemi për veten. Dave Brailsford-i e përmbledh shumë saktë përshkrimin e njerëzve që do në ekip dhe kulturën që ata duhet të përçojnë. "*Dua një kulturë urie dhe ambicieje që nuk sheh pengesa, që krijon vazhdimisht, por të organizuar e të disiplinuar, përndryshe situata mund të dalë jashtë kontrollit*".[4] Në këtë qasje, krijimtaria kërkon njerëz të vetëdisiplinuar. Pa njerëz të vetëdisiplinuar, nuk ka mundësi për punë krijuese. Puna më e vështirë është të bashkojmë disiplinën me krijimtarinë, por pa lejuar që në emër të disiplinës të pengohet krijimtaria dhe pa e lejuar krijimtarinë të shkatërrojë disiplinën.[5] Ky është një tjetër paradoks që ne duhet ta bëjmë pjesë të punës dhe kulturës sonë.

2. Krijimtaria dhe rëndësia e saj

Çdokush në vetvete është krijues. Krijimtaria është një karakteristikë e natyrshme natyrshme dhe spontane e individëve pozitivë që kanë një vlerësim të lartë ndaj vetes. Drejtuesit që krijojnë një mjedis pozitiv pune përfitojnë një rrjedhë të qëndrueshme nga të gjithë pjesëtarët e stafit. Një mori studimesh tregojnë se 95% e njerëzve shfaqin dukurinë se kanë potencial për t'i kryer punët në nivele të larta krijimtarie. Sipas kërkimeve të kryera nga Hauwrd Gardneri në Universitetin e Harvardit, studiuesit kanë dalë në përfundimin se ekzistojnë disa lloj mënyrash të ndryshme të menduari dhe se çdo person është një gjeni i mundshëm, të paktën në një lloj fushe. Ajo që kuptojmë prej kësaj është se, kyçi për t'i dhënë liri krijimtarisë tuaj zë fill nga ajo që, ju duhet të filloni dhe të mendoni për veten tuaj se jeni një person jashtëzakonisht krijues. Në librin "Roli i marketingut dhe Kreativiteti", theksohet: "Çdokush është krijues nëse e lejon veten të jetë i tillë. Është koncept i *gabuar se 'disa njerëz janë krijues'. Truri ynë ka një fuqi krijuese të jashtëzakonshme. Disa njerëz thjesht nuk janë të trajnuar për të nxjerrë në pah potencialin e tyre krijues*".[6]

---

[3] Brian Tracy, "Ndryshoni të menduarit tuaj, ndryshoni jetën tuaj, si të zbulosh potencialin tënd për sukses e arritje", Botimet Elta BS, Viti 2009, ISBN; 987-9951-544-08-5, faqe 254.

[4] Alastair Campbell, "Fitimtarët dhe si arrijnë suksesin", Shtëpia Botuese Universitare "UET Press", Tiranë 2015, ISBN: 978-9928-190-55-0, faqe 96.

[5] Vasil Naçi, Alma Bici, "Është rruga jonë, rruga e suksesit në AGNA Group", botuar nga AGNA Leadership Academy, viti 2015, faqe 114.

Të qenurit inovativ përfshin krijimtarinë në prodhimin e ideve që janë origjinale dhe të vlefshme. Ndonjëherë shfaqet një problem i ri, ose një problem i vjetër kërkon një zgjidhje të re. Drejtuesit duhet të shfrytëzojnë të tilla mundësi për të menduar në mënyrë krijuese dhe për të sjellë diçka të re. Koncepti kryesor për të menduarit krijues është zhvillimi i ideve dhe mënyrave të tjera për të nxitur vartësit me qasje dhe ide të reja.[7] Në këtë kuadër, krijimtaria dhe inovacioni mbështesin njëra-tjetrën. Organizatat përballen me një dilemë: nëse nuk krijojnë risi ato nuk mund të mbijetojnë. Por edhe nëse krijojnë risi dhe ato nuk rezultojnë të suksesshme, organizatat përsëri nuk mund të mbijetojnë. Për këtë arsye, krijimtarinë dhe inovacionin duhet ta bëjmë pjesë të punës sonë të përditshme. Idetë e mira nuk vijnë çdo ditë dhe jo çdo ide mund të jetë e suksesshme, por organizatat që vjetrohen në ide dhe ndalen së krijuari, janë të destinuara të dalin përfundimisht nga misioni.

Krijimtaria dhe inovacioni duhet të bëhen mendësi dhe zakon pune. "*Më të suksesshmit e të suksesshmëve* – thekson G. Cardone, - *shkojnë përtej konceptit të ndryshimit dhe sfidojnë mendësinë tradicionale. Vështroni organizatat si Google, Apple dhe Facebook, e do të vëreni kompani që sfidojnë traditat dhe krijojnë mënyra të reja për t'i bërë gjërat. Ata e thyejnë atë çfarë tashmë funksionon, në mënyrë që të përmirësojnë. Më të suksesshmit kërkojnë të krijojnë tradita të reja – jo të ndjekin ato që tashmë ekzistojnë. Mos u bëni një i burgosur i mendësisë së rënë dakord prej të tjerëve. Zbuloni mënyra për të shfrytëzuar në maksimum mendësinë tradicionale e cila pengon të tjerët*".[8] Prandaj është e rëndësishme të jemi më krijues se konkurrentët tanë. Në ditët e sotme teknologjia dhe inovacioni kanë krijuar një botë të re. Për të ruajtur avantazhet konkurruese, një organizatë duhet të vlerësojë jashtëzakonisht rolin e krijimtarisë. Përdorimi i krijimtarisë në prodhim, pajisje, kosto dhe në të gjitha aspektet e tjera, jo vetëm që ndihmon organizatën që të rritet, por gjithashtu krijon përparësi, krahasuar me të tjerat. Një organizatë ka nevojë për fuqinë krijuese të njerëzve për të përballuar sfidat e kohës. Idetë janë motorrët e progresit. Ato përmirësojnë jetën e njerëzve duke krijuar mënyra më të mira për të bërë gjërat. Ato ndërtojnë dhe rrisin organizatat e mëdha duke i mbajtur ato gjithmonë të suksesshme.

---

[6] Vasil Naçi, Alma Bici, "Roli i marketingut dhe Kreativiteti", botuar nga Agna Leadership Academy, Viti 2012, faqe 93.

[7] FM 6-22, Army Leadership Competent, Confident, and Agile, October 2006, faqe 6-2.

[8] Grant Cardone, "10 X: Rregulli i vetëm që bën dallimin ndërmjet suksesit dhe dështimit", Shtëpia Botuese "Minerva", Viti 2020, ISBN: 978-9928-2611-2-8, faqe 187.

Aftësia jonë gjeniale për krijimtarinë qëndron në fuqinë për të rikombinuar dhe integruar me freski elementet ekzistuese. Krijimtaria është vepër e gjimnastikës mendore dhe përfshin pjesën ndërgjegjësore të trurit. Ai tërheq gjithçka nga njohuritë, logjika, imagjinata, intuita e deri tek aftësia për të parë lidhjet dhe dallimet mes ideve dhe gjërave.

Meqë shumica e proceseve dhe sistemeve tona edukuese i janë përkushtuar zhvillimit të funksionit të të menduarit gjykues (aftësisë për të marrë vendime, për të krahasuar dhe vlerësuar situatat, për të bërë dallimin midis së duhurës dhe jo korrektes etj.,) shumë njerëz nuk e kuptojnë fuqinë e aftësive krijuese vetjake. Në të vërtetë, potenciali ynë në këtë fushë është përherë i pranishëm dhe mund të zhvillohet në masë shumë më të madhe tejet lehtësisht. Asnjëherë nuk duhet ta humbim besimin në aftësitë tona krijuese.[9] Krijimtaria kërkon përkushtim, dedikim, orë të gjata dhe vazhdimisht njohuri të reja. Si në çdo aspekt të jetës, pa pasion dhe dashuri për krijimtarinë, asgjë e madhe nuk mund të ndodhë. Nëse keni shpirtin krijues, ju do të gjeni ide të reja ndërkohë që jeni duke përmbushur detyrat tuaja të përditshme.

Aftësia për të menduar në mënyrë krijuese, për t’i analizuar problemet dhe mundësitë në mënyra të reja dhe inovative, përbën një nga zotësitë më të vyera që mund të zhvillojmë në vetvete dhe brenda organizatës sonë. Për këto arsye, krijimtaria merr rëndësi të veçantë sepse:

- rrit produktivitetin, sjell gëzim, rrit kënaqësinë, ju mban të freskët, ju bën më konkurrues dhe e ndihmon organizatën të rritet, duke pasur në vijimësi avantazhet e nevojshme;
- i jep kuptim jetës, ju jep fuqi të provoni qasje të reja, ju mban zgjuar, ju ndihmon të bëheni më elastikë e më të përshtatshëm;
- ju çon në rezultate shumë të mira përmes një përqasjeje tjetër që askush nuk e ka parë më herët, duke e bërë kontributin dhe suksesin tuaj origjinal dhe unik.

---

[9] Dale Carnegie & Associates, “Si të bëhesh udhëheqës i zoti”, Shtëpia Botuese “Pema”, Viti 2019, ISBN: 978-9951-721-77-6, faqe 175.

- ju ndihmon të gjeni mjete të reja për të arritur rezultatet.
- ndihmon organizatën të bëjë vetë progres.

3. Karakteristikat e njerëzve që mendojnë në mënyrë krijuese

Të menduarit krijues është procesi i përdorimit të trurit për të gjeneruar ide rreth diçkaje. Krijimtaria duhet të sjellë rezultate cilësore. Të menduarit krijues do të thotë ide cilësore për problemin, për t'i dhënë organizatës një energji më të madhe. Sipas Michael Schrage-it *krijimtaria e vërtetë nuk ka të bëjë vetëm me idetë. Ka të bëjë me përkthimin e ideve në produkte, shërbime dhe zgjidhje të zgjuara.*[10] Ka vend për krijimtari në çdo aspekt të jetës. Krijimtaria dhe epërsia (përsosmëria) janë të lidhura ngushtë me njëra-tjetrën. Ata që dëshirojnë më të mirën, duhet ta bëjnë krijimtarinë mënyrë jetese. Walt Disney thotë se nëse ëndërron diçka, mund ta bësh.

Aftësitë krijuese janë "ar i kulluar", pavarësisht se çfarë pune bën në jetë. Annette Moser-Wellman, autore e librit "The Five Faces of Genius, thotë: "*Pasuria më e vlefshme që mund t'i sjellësh punës dhe organizatës janë aftësitë e tua krijuese. Ajo që ka më shumë rëndësi, krahasuar me atë se çfarë bën, me rolin që luan, me titullin që mban, me rezultatin që jep – janë idetë e tua*"[11]. Pavarësisht rëndësisë që ka zotësia e dikujt për të menduar me aftësi krijuese, duket se shumë pak veta e kanë këtë zotësi me bollëk.

Njerëzit krijues, asnjëherë nuk janë të kënaqur me atë që kanë arritur. Ata kërkojnë zgjidhje të reja të problemeve. Kanë një dëshirë të fortë për të krijuar, kanë ndjenjë të thellë përgjegjësie dhe qartësie për qëllimet që duan të arrijnë. Kanë durim dhe përqendrim, janë elastikë, kanë ndjeshmëri ndaj problemeve, janë kureshtarë. Parë në këtë këndvështrim, karakteristikat më tipike të njerëzve krijues janë:

Njerëzit krijues i vlerësojnë idetë. Annette Moser-Wellman vërejti: "*Njerëzit me një mënyrë të menduari tepër krijuese janë të përkushtuar ndaj ideve. Ata nuk mbështeten vetëm në talentin, por edhe në disiplinën e tyre. Imagjinata është si një lëkurë e dytë për ta. Dhe dinë si ta përdorin në masën më të plotë*".[12] Të kesh aftësi krijuese, do të thotë të kesh ide, shumë ide. Do të keshide vetëm nëse i vlerëson ato.

Njerëzit krijues eksplorojnë mundësitë. Eksplorimi i sa më shumë mundësive stimulon imagjinatën dhe imagjinata është thelbësore për aftësinë krijuese. Sikurse thotë Albert Ajnshtajni, imagjinata është më e rëndësishme se njohuria. Në këtë kuadër, njerëzit duhet të vlerësojnë shumë mundësitë, pasi ato kanë çelësin për të gjetur përgjigjet më të mira, jo përgjigjen e vetme. Ata që dinë të mendojnë, gjejnë përgjigjet më të mira. Ata krijojnë plane rezervë që u japin alternativat. Ata gëzojnë një liri që të tjerët nuk e zotërojnë. Kështu ata do të kenë ndikim tek të tjerët dhe do t'i udhëheqin.

---

[10] Vasil Naçi, Alma Bici, "Roli i marketingut dhe Kreativiteti", botuar nga Agna Leadership Academy, Viti 2012, faqe 89.

[11] John C. Maxwell, "Si mendojnë njerëzit e suksesshëm" Shtëpia Botuese "Bota shqipëtare", Tiranë 2020, ISBN: 978-9928-00-455-0, faqe 65.

[12] Po aty, faqe 67.

Njerëzit krijues janë të hapur ndaj interpretimeve të ndryshme. Shkrimtari H. L. Mencken thotë se njeriu mendjelehtë është gjithmonë i sigurt dhe njeriu i sigurt është gjithmonë mendjelehtë. Njerëzit me aftësi krijuese nuk e ndiejnë nevojën për të përjashtuar pasiguritë. Ato i shohin të gjitha mospërputhjet dhe hendeqet e jetës, dhe shpesh kënaqen t'i eksplorojnë këto hendeqe, apo të përdorin imagjinatën për t'i mbyllur këto hendeqe.

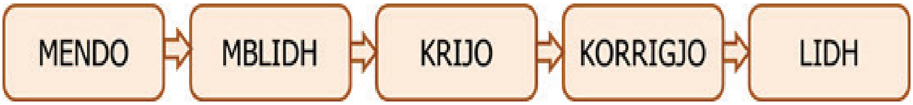
Njerëzit krijues i ngazëllon e pazakonta. Është në vetë natyrën e aftësive krijuese që shpesh eksplorojnë përtej shtigjeve të zakonta dhe të shkojnë kundër rrymës. Diplomati dhe presidenti për një kohë të gjatë i Universitetit Yale, Kingman Brewster, thekson se ekziston një lidhje mes aftësive krijuese dhe çmendurisë, prandaj duhet ta durojmë me gëzim çmendurinë. Që të ushqesh aftësi krijuese te vetja ose te të tjerët, mos ki merak të jesh dhe pak i çuditshëm. Ja një shembull domethënës: Në vitin 1878, Thomas Edisoni nuk ishte i vetmi që eksperimentonte me llamba inkandeshente, por ishte i vetmi që provoi 6.000 filamente të ndryshme; në këtë mënyrë, ai përparoi milimetër pas milimetri derisa zbuloi zgjidhjen përfundimtare. Dhe sigurisht, më në fund e gjeti këtë zgjidhje, duke dëshmuar se gjenialiteti është shpesh, thjesht çështja e këmbënguljes së maskuar.[13] Duke shfrytëzuar gjithë forcën e tij fizike dhe mendore, duke mos u lodhur kurrë dhe duke mos hequr dorë për asnjë çast, Edisoni iu rezistoi konkurrentëve të paduruar, kur zbuloi në një copë bambuje mënyrën se si të ndriçonte botën.

Njerëzit krijues lidhin ato që duket se s'kanë lidhje. Ngaqë aftësitë krijuese përdorin idetë e të tjerëve, është shumë e vlefshme të jesh në gjendje të lidhësh idetë me njëra – tjetrën, sidomos ato ide që duket sikur s'kanë lidhje. Dizajneri grafik Tim Hansen thotë: "*Aftësitë krijuese shprehen veçanërisht në zotësinë për të bërë lidhje, për të bërë shoqërizime, për t'iu rikthyer gjërave e për t'i shprehur ato në një mënyrë të re*"[14]. Të menduarit në mënyrë krijuese është pak a shumë kështu:

---

[13] Ryan Holiday, "Pengesa është rrugëdalja", Shtëpia Botuese "Minerva", Tiranë 2019, ISBN: 978-9928-265-13-5, faqe 90.

[14] John C. Maxwell, "Si mendojnë njerëzit e suksesshëm" Shtëpia Botuese "Bota shqipëtare", Tiranë 2020, ISBN: 978-9928-00-455-0, faqe 69.



Kur ia nis të mendosh, je i lirë të mbledhësh. Pyet veten: Çfarë materiali ka lidhje me këtë ide? Pasi të kesh gjetur materialin pyet: *Cilat ide mund të më ndihmojnë të mendoj më mirë?* Kështu mund të fillosh të ngresh idenë në një nivel tjetër. Pas kësaj mund të korrigjosh ose të qartësosh duke pyetur: *Cilat ndryshime mund ta përmirësojnë këtë ide?* Së fundi, lidhi idetë, duke i vendosur në kornizën e duhur për ta bërë mendimin të plotë e të fuqishëm.

Njerëzit krijues nuk kanë frikë nga dështimi. Aftësia krijuese kërkon të kesh zotësinë për të mos pasur frikë nga dështimi, sepse të krijosh është baras të dështosh. Charles Frankel pohoi se ankthi është gjendja thelbësore e krijimit intelektual dhe artistik. Ndërsa Steve Jobs-i është më i drejtpërdrejtë kur pohon: *"Ndonjëherë, kur ju jeni novator, ju bëni gabime. Mënyra më e mirë është që t'i pranoni ato shpejt dhe t'i futeni punës për të përmirësuar risitë e tjera."*[15]

4. Krijimtaria, detyrë drejtuese

Aftësi për të krijuar e marrë vendime është një kualifikim kyç për drejtuesin. Drejtuesi ushtarak duhet t'u japë rrugëzgjidhje bindëse dhe rezultative problemeve. Kjo do të realizohet nëse ai ka aftësi të mira për të krijuar dhe marrë vendime të drejta. Aftësia për të krijuar, krahas të tjerave evidentohet: në përcaktimin e strukturave të reja për të përballuar situatat dhe zgjidhjen e problemeve; në aftësinë për të braktisur modelet e vjetra të drejtimit; në aftësinë për të përballuar volumin e detyrave gjithnjë në rritje; në rolin e tij si moderator i konferencave apo debateve të përcaktuara, ku të gjejnë zbatim rregullat e normat e punës së grupeve joformalë. E thënë ndryshe, në aftësinë për t'i lënë hapësirën e nevojshme vartësve në diskutime e debate, duke fituar argumenti dhe jo pozicioni si drejtues. Kjo do të thotë që vartësve t'u hiqet tutela e drejtuesit dhe ata të jenë të lirshëm në dhënien e ideve e mendimeve, pa pasur "frikën" e nënqeshjes (shpotisë) apo ndëshkimit. Referuar Charlie Brower-it: "*Një ide e re është delikate. Atë mund ta vrasësh me një tallje a një thumb; mund ta presësh për vdekje me një nënqeshje e ta kërcënosh me vdekje me një ngrysje vetullash në ballin e njeriut të duhur*".[16] Mjediset negative vrasin çdo minutë mijëra ide të mëdha. Në krahun tjetër, një mjedis krijues bëhet si një serrë ku idetë mund të mbillen, të çelin syth e të lulëzojnë. Për këtëarsye drejtuesi duhet të shohë "peshën" e përfitimeve të organizatës kur ai arrin të përshtatet me ndjenjat e bashkëpunëtorëve të tij, të dijë si të përballet me mosmarrëveshjet në mënyrë që ato të mos përshkallëzohen, duke krijuar lehtësira që stafi përkatës të punojë me ritmin e duhur dhe pa stres. Aftësia për të drejtuar nuk do të thotë të sundosh të tjerët, por t'i bindesh të përpiqen për arritjen e qëllimit të përbashkët.[17] Është detyrë e drejtuesit që të zotërojë aftësitë për të kuptuar thellë vartësit, që padyshim janë të lidhur me detyrën dhe me ndryshimet që duhet të ndërmarrin në mënyrë që puna të japë më shumë kënaqësi.

---

[15] Bryan Tracy, "Kreativiteti dhe zgjidhja e problemeve" Shtëpia Botuese "Damo", Prishtinë 2015, ISBN: 978-9951-642-38-5, faqe 101.

[16] John C. Maxwell, "Si mendojnë njerëzit e suksesshëm" Shtëpia Botuese "Bota shqiptare", Tiranë 2020, ISBN: 978-9928-00-455-0, faqe 79.

Receta e suksesit për një drejtues kërkon: së pari, të krijojë reputacionin e njeriut krijues; së dyti, të rrethojë veten me bashkëpunëtorë që janë më të mirë se ai; së treti, t'i lërë ata të bëjnë punën. Pra aftësia për të krijuar, krahas krijimtarisë vetjake të drejtuesit, shihet edhe në metodologjinë e ndjekur prej tij për të shfrytëzuar aftësitë krijuese të vartësve e të bashkëpunëtorëve në të mirë të realizimit të detyrës, objektivit, misionit. Për këtë drejtuesi herë pas here duhet të pyesë vartësit e vet: "Si mund të të ndihmoj, si të ta lehtësoj më tej punën? Ç'praktikë e imja ta bën punën të vështirë. Ç'vendime e ç'stil të shqetësojnë vërtet ty?" Në qoftë se drejtuesi nuk i bën të tilla pyetje ai vetëm sa do t'i prekë problemet, por nuk do t'i zgjidhë ato. Ju si drejtues mund të mendoni se po bëni një punë të madhe, ndërsa të tjerët në organizatë mund të harxhojnë mjaft kohë për të pakësuar pasojat e gabimeve tuaja. Prandaj, drejtuesi duke qenë vazhdimisht në kontakt me vartësit, duke ndjekur në vijimësi problemet, duke konstatuar çfarë shkon e çfarë nuk shkon, është në gjendje të krijojë situata të favorshme që mbështesin punën e vartësve aftësitë e tyre krijuese, të krijojë procedura të reja me qëllim që çdo gjë të kryhet e zbatohet sipas rregullave, normave e procedurave përkatëse.

Drejtuesit, gjithmonë duhet të jenë krijues të hapur. Drejtues të mirë janë vetëm ata mendja e të cilëve kurrë nuk mbyllet, ata të cilët janë të interesuar të dëgjojnë ide e pikëpamje të reja, që i hyjnë me zell zgjidhjes së çështjeve të reja[18]. Për shembull, edhe kur janë marrë vendimet një drejtues duhet të jetë i gatshëm të dëgjojë mendimet e kundërta dhe të vlerësojë ndryshimet dhe kushtet e reja që janë krijuar. Drejtuesit nuk duhet të ndryshojnë vazhdimisht mendjen, pasi kanë marrë një vendim të madh, por në qoftë se nuk vlerësojnë situatën, ata do të tregojnë kokëfortësi dhe intolerancë, të cilat do të sjellin shqetësime për organizatën.

---

[17] Daniel Goleman, "Inteligjenca emocionale, Shtëpia Botuese "Pema", Prishtinë 2018, ISBN: 978-9951-721517, faqe 182.

[18] Perri Smith, "Përgjegjësia", Shtëpia Botuese e Ushtrisë, Tiranë 1994, faqe 31.

Marrja e vendimit është një çast shumë i rëndësishëm në veprimtarinë krijuese dhe drejtuese, pasi ai është thelbi në bazë të të cilit do të planëzohet vijueshmëria e tërë punës së mëpastajme. Prandaj drejtuesi duhet të kuptojë dhe zotërojë procesin e marrjes dhe të zbatimit të vendimit. Si merren vendimet? Çfarë metodologjie ndiqet për t'i marrë ato? Ç'vendime lënë që t'i marrin vartësit? Cilat vendime duhet të miratojnë ata në autoritetin më të lartë? Këto janë disa lloj pyetjesh, të cilave drejtuesit duhet t'u japin përgjigje. Ata duhet të dinë gjithashtu si të zbatojnë vendimet sepse ato bëhen të pavlefshme në qoftë se mbesin vetëm në letër. Kjo është dhe arsyeja që drejtuesit duhet të dinë të zhvillojnë strategjinë e zbatimit. Ata duhet të gjejnë rrugën që vendimet të zbatohen me çdo kusht, të zbatohen me krijimtari në formë e në përmbajtje.

Një drejtues i mirë, angazhon stafin e tij në marrjen e vendimit, duke e moderuar konsultën në mënyrë të tillë, që të rezultojë kursi më i saktë i veprimit dhe vendimi të jetë produkt i stafit të vartësve dhe bashkëpunëtorëve, ku padyshim pjesëtar është edhe drejtuesi. Kjo bën që për zbatimin e plotë të çdo vendimi të kesh gjithmonë mbështetjen e padiskutueshme të vartësve të tu, që ju i keni angazhuar me maturi e profesionalizëm, duke u lënë në dorë hapësirën e nevojshme dhe fushën e përgjegjësisë për të dhënë idetë, mendimet e tyre dhe për të bërë vlerësimet përkatëse. Një sesion i zhvilluar për marrjen e vendimit është pothuajse i ngjashëm me "stuhi mendimesh"[19], pasi përcaktimi i saktë i kurseve të veprimit kërkon shumë ide, pas kësaj bëhen analiza, gjykime, këndvështrime të ndryshme, seleksionime, lidhje të atyre të mbetura e deri sa arrihet përfundimi i duhur. Edhe në këtë proces është shumë e rëndësishme që të gjejnë zbatim kriteret e Osbornit[20] dhe kjo është përgjegjësi e drejtuesit.

Në qoftë se vartësve u jepet mundësi e plotë për të shprehur pikëpamjet e tyre para se të merret vendimi, ata do të jenë të gatshëm për ta zbatuar atë edhe sikur vendimi të mos jetë ai që do të kishin dashur ata. Kjo është e lidhur dhe me klimën dhe besueshmërinë e dyanshme midis drejtuesit dhe të drejtuarve. Gjenerali C. Powell-i e shpjegon thjesht këtë dukuri: "*Kur jemi duke debatuar për një çështje besnikëri do të thotë të më jepni mua opinionin tuaj të ndershëm,*

---

[19] Koncepti "Stuhia e mendimeve" (brainstorming) jepet për herë të parë nga Alex Osborn-i, qysh nga fillimi i vitit 1939. Ai është një personazh legjendar i reklamave të viteve 40 të shekullit të kaluar. Për Osbornin, zgjidhja nuk ishte që vartësit të punonin të pavarur, por të shmangej kritika në grup. Kështu, ai krijoi konceptin "Stuhi mendimesh", një proces gjatë të cilit pjesëtarët e grupit sjellin ide në një mjedis aspak gjykues. Teoria e Osbornit pati ndikim të madh për kohën dhe u përqafua me entuziazëm nga drejtues të ndryshëm kompanish. (Shënimi i autorit)

[20] Katër rregullat bazë të konceptit "Stuhia e mendimeve" janë: 1. Mos i gjyko ose kritiko idetë e të tjerëve; 2. Shprehu i lirshëm, sa më e zgjuar ideja, aq më mirë; 3. Sasia është e rëndësishme, sa më shumë ide, aq më mirë; 4. Krijo ide të reja, mbështetur tek ato të kolegëve. (Susan Cain, "Pushteti i të heshturve", Shtëpia Botuese "Living", Tiranë 2019, ISBN: 978-9928-216-59-5, faqe 92-93)

sido që ta mendoni, në e pëlqej unë apo jo. Mendimet e ndryshme në këtë fazë më stimulojnë mua. Por sapo të jetë marrë vendimi, debati mbaron. Që nga ky çast e tutje besnikëri do të thotë zbatimi i vendimit, sikur atë ta kishit marrë vetë”[21].

Kjo metodë nuk vlen vetëm për nxitjen e ideve risi nga të tjerët, por është edhe një lloj prirjeje për të mbajtur mendjen të hapur. Jo më kot, Gjenerali amerikan Xhorxh Patoni këshillonte: “…*Mos u thuaj kurrë njerëzve si t’i bëjnë gjërat. Thuaju atyre vetëm çfarë duhet të bëjnë dhe ata do të të habisin me mendjemprehtësinë e* tyre”[22]. Drejtimi duke qenë imponim vullneti tek të tjerët është veprimtari e një grupi njerëzish të cilët duhen orientuar drejt prioriteteve kryesorë. Prandaj për drejtuesin është parësore njohja dhe përdorimi i parimeve të punës në grup duke gërshetuar me kujdes modelin e të menduarit me teknikat përfytyruese. Por gjithsesi, të krijosh dhe të marrësh vendime do të thotë të kesh një strategji të qartë mendimi, qëndrimi dhe sjelljeje. Aftësia për të krijuar e marrë vendime është një kualifikim kyç që kërkon të kuptosh e të konceptosh se mësohet çdo ditë dhe krijohen ide, mendime, si dhe përcaktohen metodologji apo metoda efikase për të vepruar me efikasitet dhe për të pasur sukses.

Përfundime

Krijimtaria është një proces i rëndësishëm për drejtuesin dhe organizatën pasi është i lidhur me suksesin dhe jetëgjatësinë e saj.

Një drejtues, një përqindje të caktuar të kohës së tij e kalon duke zgjidhur probleme vetë ose bashkë me të tjerët, që i shërbejnë drejtpërsëdrejti punës. Aftësia drejtuese për t’u përballur me vështirësitë dhe për t’i zgjidhur problemet, do të përcaktojë më shumë se çdo gjë tjetër, gjithçka që ndodh në karrierën e tij dhe në ecurinë e organizatës që drejton.

Megjithëse, krijimtaria është përgjegjësi e gjithsecilit, drejtuesi duhet të krijojë një mjedis të hapur që ta nxisë atë, ku secili të shfaqë talentin e tij krijues, duke orientuar të gjithë energjitë e tyre në përmbushjen e misionit. Ajo triumfon kur kemi kulturën që fuqizon procesin krijues. Krijimtaria nuk duhet të ndodhë vetëm njëherë apo në mënyrë sporadike. Mendo në mënyrë krijuese, rri me njerëz që janë krijues dhe përfshihen në procese krijuese. Kështu ju mund të ndani me ta pasionin për krijimtari dhe ta forconi këtë pasion. Shpërbleni krijimtarinë. Bëjini njerëzit të ndihen që po bëjnë një punë të shkëlqyer. Inkurajojini të bëjnë më shumë.

---

[21] Kolin Pauell, “Udhëtimi im amerikan”, Shtëpia Botuese e Ushtrisë, Tiranë 1999, faqe 237.

[22] Perri Smith, “Përgjegjësia”, Shtëpia Botuese e Ushtrisë, Tiranë 1994, faqe 22.

Njerëzit krijues nuk janë të kënaqur me atë që kanë arritur. Ata, vazhdimisht kanë pritshmëri të larta, duke kërkuar zgjidhje të reja problemore. Ata kanë qartësi për atë që dëshirojnë të arrijnë, dinë të ndërthurin gjykimin me fantazinë, kureshtjen me elasticitetin për të dhënë zgjidhjet e duhura, për të shmangur pengesat e ndryshme dhe për ngritur "stekën" e standardeve.

Krijimtaria është proces i pafund. Drejtuesi, nëpërmjet strukturave përkatëse duhet të inkurajojë dhe të mbështesë idetë e reja; duhet të parashikojë një buxhet për të investuar në projektet e reja premtuese; duhet të tërheqë talentet e nevojshëm për të zbatuar këto ide.

Hapësira të pafundme për aspektet e reja, këputja e "prangave" dhe braktisja e zakoneve "të dashura" të rutinës së përditshme, për të siguruar rrugë të lirë për shndërrime të reja e të suksesshme është një çështje parimore në veprimtarinë krijuese. Dhuntia krijuese e njerëzve duhet të përcaktojë drejt gjykimin e qëllimit dhe zgjidhjen e problemit, si dhe shmangien e propozimeve jo të rëndësishme. Personeli dhe përmasat specifike të grupeve të punës si dhe strukturat e tyre, ndikojnë drejtpërsëdrejti mbi krijimtarinë.

Për të inkurajuar krijimtarinë dhe inovacionin brenda organizatës, gjithashtu duhet të evidentohen disa faktorë me rëndësi të veçantë: këto kanë të bëjnë me elemente njerëzorë brenda organizatës, si respekti, besimi, përkushtimi dhe mirënjohja.

Bibliografia

1. Susan Cain, "Pushteti i të heshturve", Shtëpia Botuese "Living", Tiranë 2019, ISBN: 978-9928-216-59-5.
2. Alastair Campbell, "Fitimtarët dhe si arrijnë suksesin", Shtëpia Botuese Universitare "UET Press", Tiranë 2015, ISBN: 978-9928-190-55-0.
3. Grant Cardone, "10 X: Rregulli i vetëm që bën dallimin ndërmjet suksesit dhe dështimit", Shtëpia Botuese "Minerva", Viti 2020, ISBN: 978-9928-2611-2-8.
4. Dale Carnegie & Associates, "Si të bëhesh udhëheqës i zoti", Shtëpia Botuese "Pema", Viti 2019, ISBN: 978-9951-721-77-6.
5. Daniel Goleman, "Inteligjenca emocionale, Shtëpia Botuese "Pema", Prishtinë 2018, ISBN: 978-9951-721-51-7.
6. Ryan Holiday, "Pengesa është rrugëdalja", Shtëpia Botuese "Minerva", Tiranë 2019, ISBN: 978-9928-265-13-5.
7. John C. Maxwell, "Si mendojnë njerëzit e suksesshëm" Shtëpia Botuese "Bota shqipëtare", Tiranë 2020, ISBN: 978-9928-00-455-0.

8. Vasil Naçi, Alma Bici, "...Është rruga jonë, rruga drejt suksesit në Group", botuar nga Agna Leadership Academy, Viti 2015.
9. Vasil Naçi, Alma Bici, "Roli i marketingut dhe Kreativiteti", botuar nga Agna Leadership Academy, Viti 2012.
10. Brian Tracy, "Kreativiteti dhe zgjidhja e problemeve" Shtëpia Botuese "Damo", Prishtinë 2015, ISBN: 978-9951-642-38-5.
11. Brian Tracy, "Ndryshoni të menduarit tuaj, ndryshoni jetën tuaj, si të zbulosh potencialin tënd për sukses e arritje", Botimet Elta BS, Viti 2009, ISBN; 987-9951-544-08-5.
12. Q. Orhani, E. Braneshi, M. Cukalla, "Udhëheqja Ushtarake 2", shtypur në Shtypshkronjën "Grand Prind", Tiranë 2011.
13. Kolin Pauell, "Udhëtimi im amerikan", Shtëpia Botuese e Ushtrisë, Tiranë 1999.
14. Perri Smith, "Përgjegjësia", Shtëpia Botuese e Ushtrisë, Tiranë 1994.
15. FM 6-22, Army Leadership Competent, Confident, and Agile, October 2006.

Përgatitja dhe zhvillimi i oficerëve të sotëm për mënyrat e reja të luftës së nesërme

Nënkolonel (R) Msc. Besnik DACI
Specialit në IKSHU

Trajtesë e shkurtuar.

Natyra e re ndryshuese e luftës dhe e konflikteve në shekullin e 21-të, kërkojnë të transformojmë zhvillimin e drejtuesve ushtarak, për t'i përgatitur me sukses, për luftëra të reja që vendi ynë mund të përballet në të ardhmen.

Qëllimi është të edukojmë oficerë dhe të përcjellim tek ata aftësitë e duhura, për realizimin me sukses të misionit dhe detyrat themelore të FA, në kryerjen e spektrit të plotë të operacioneve ushtarake, në kuadër të angazhimeve kombëtare e ndërkombëtare, të "Armatosur" me strategji, që mendojnë në mënyre kritike dhe mund të aplikojnë ide të reja, në fuqinë ushtarake për të kontribuar në strategjinë e sigurisë kombëtare dhe atë ushtarake dhe për të luftuar në të gjitha kushtet dhe rrethanat.

Kjo temë, ofron vizionin e përgatitjes dhe zhvillimit të oficerëve të sotëm për mënyrat e reja të luftës së nesërme, për rezultatet që kërkohen, ju ofron udhëzime për t'i arritur ato. Ka si synim të udhëheqë zhvillimin e strategjive të reja të drejtuesve, ofrimin e talenteve dhe menaxhimin e tyre, si dhe të formojë drejtues ushtarak të niveleve të ndryshme për nevoja të kombit.

Fjalë kyçe: Arsimi Ushtarak Profesional (AUP); Arti i luftës; fuqia ushtarake; qasje shtrirëse dhe holistike; forca e përbashkët; forca e përbashkët e bashkuar; elitë ushtarake; operacione të integruara; inovacion; sinergji.

1. Zhvillimi i oficerëve të sotëm për mënyrat e reja të luftës së nesërme

Për të mbrojtur arritjet tona të deritanishme dhe aftësitë për tu përshtatur e për të synuar vlerat më të mira jo vetëm kombëtare por edhe më tej, duhet që më shumë se sa blerja e pajisjeve ushtarake; të fitojmë dhe të mbajmë përparësitë intelektuale. Gjithashtu, duhet të aplikohet komunikimi dhe efektshmeria e forcës në mënyrë të përshtatshme për të parandaluar, luftuar dhe fituar kundër kundërshtarëve tanë. Kjo nuk mund të arrihet pa përmirësimin e konsiderueshëm të kapaciteteve zbuluese të luftëtarëve të përbashkët, për të krijuar, projektuar dhe zbatuar strategji integruese, për të treguar aftësitë tona përkrah vendeve të NATO-s, për të sfiduar kundërshtarët që sjell koha, dhe për të reaguar ndaj aktiviteteve që nuk sjellin konflikte të armatosura.

Shekulli i 21-të kërkon që oficerët tanë të jenë më shumë të arsimuar dhe më të aftë për të drejtuar dhe integruar instrumentin ushtarak të kombit tonë. Kapacitetet intelektuale të përshkruara më lartë zhvillohen gjatë një karriere dhe jo si rezultat i mundësive edukative episodike, sidomos kur ato mundësi nuk janë as aktuale as rigoroze. Përkundrazi, këto aftësi përmirësohen gjatë mijëra orësh praktike dhe pune, duke zgjeruar kufijtë njohës dhe performancën intelektuale.

Karriera e një oficeri duhet të jetë e dizajnuar për të zhvilluar, përshtatur dhe ushtruar vazhdimisht aftësi intelektuale të reja, sidomos në ecurinë e karrierës e deri në gradat më të larta.

Për të arritur qëllimin për zhvillim të drejtuesve, nevojitet një trajektore e re për Arsimimin Ushtarak Profesional, (AUP) që duhet të përfshijë sisteme të lidhura të menaxhimit të talenteve. Vizioni duhet të jetë për një AUP dhe sistem të plotë të menaxhimit të talenteve, që identifikojnë, zhvillojnë dhe përdorin lidership me strategji, të cilët mendojnë në mënyrë kritike dhe kreative në artin e luftës dhe në aplikimin praktik dhe etik të fuqisë luftarake.

2. Mjedisi i sigurisë dhe operacionet globale të integruara

Deri më tani, programet tona të AUP kanë prodhuar oficerë që i kanë shërbyer me nder vendit tonë dhe Forcës së Përbashkët në strukturat e NATO-s. Strategjia e Sigurisë Kombëtare dhe Strategjia Ushtarake bëjnë të qartë se mjedisi ynë i sigurisë po ndryshon. Kthimi i konkurrencës së fuqishme rrit stërvitjen dhe inovacionin. Ndërsa ndryshimi është i përbashkët në kuptimin tonë të karakterit të luftës, shpejtësia e rritjes dhe konvergjenca e teknologjive të reja parashikon ndryshime dramatike në mënyrën se si zhvillohen konfliktet dhe, kështu, kërkon ndryshim të thellë në mënyrën tonë për të planifikuar dhe ekzekutuar operacionet. Për të arritur suksesin në parandalimin ose fitimin e konflikteve të ardhshme, ne duhet të adaptojmë gjithashtu ndjeshëm shërbimin tonë të zhvillimit të drejtuesve dhe të mos shmangemi nga ndryshimet themelore kur të jetë e nevojshme. Për Forcën e Armatosur, ndryshimet në karakterin dhe kryerjen e luftës dhe operacioneve kërkojnë:

- Integrim të vazhdueshëm të instrumenteve kombëtare të pushtetit dhe ndikimit në mbështetje të objektivave kombëtare;
- Mendim kritik, strategji në gjithë spektrin dhe struktura të tjera të përbashkëta.
- Përdorim qasje kreative për luftën në mbrojtjen e vendit dhe fushatat e përbashkët me aleatët;
- Bashkëpunim dhe integrim të efektshëm i koalicionit, me aleatët, partnerët ndërkombëtarë dhe Shtetet e Bashkuara të Amerikës në veçanti;
- Kuptimi më i thellë i pasojave të teknologjive të rrezikshme dhe të ardhshme për kundërshtarët dhe veten tonë.

Këto kërkesa intelektuale në zhvillimin aktual të drejtuesve tanë nuk kanë qenë fokusi ynë i vetëm. Ne mund të bëjmë më të mirën në lidhje me zgjedhjen e studentëve tanë, shkollën ku ata studiojnë dhe çfarë ata mësojnë aty, profilet e tyre, dhe detyrat e tyre të mëtutjeshme. Ne duhet të përcjellim mendim kritik dhe kreativ, mësim të vazhdueshëm dhe zhvillim profesional, të identifikojmë bashkërisht detyrat e mëtutjeshme që vazhdojnë të ushtrojnë dhe ndërtojnë kapitalin intelektual të rikrijuar përmes AUP-së. Vendit tonë i nevojiten liderë luftarakë dhe oficerë stafi të aftë për të zhvilluar dhe udhëhequr në një mjedis dinamik, globalisht të integruar. Ne nuk mund të mbështetemi thjesht në masë ose në teknologjinë më të mirë. Sot dhe në të ardhmen, teknologjia mund të jetë në duart e kundërshtarëve tanë. Puna jonë është të mësojmë si të aplikojmë aftësitë tona më mirë dhe në mënyre me kreative.

Këto kërkesa rrisin kërkesat në vazhdimësinë e zhvillimit të drejtuesve tanë që ende nuk i plotësojmë. Thjesht, ne kërkojmë liderë në të gjitha nivelet që mund të arrijnë nivelin apo mbizotërim intelektual kundër kundërshtarëve. Për të arritur këtë, duhet inovacion dhe përshtatja nëpërmjet programeve tona AUP, dhe përpjekjeve të menaxhimit të talenteve për të zhvendosur politikat tona, sjelljet dhe kulturat në përputhje me ndryshimin e karakterit të luftës. Kapacitetet njohëse që këta drejtues sjellin në operacionet e integruara globalisht nuk janë thjesht produkt i një kursi 10-mujor; ato janë produkt i një Etosi (karakteri) të zhvillimit profesional të qëndrueshëm gjatë karrierës dhe një vazhdimësie të edukimit/mësimit.

3. Stadet e preferuara të vazhdimësisë së mësimdhënies

Zhvillimi i liderëve kërkon një qasje shtrirës dhe holistike[1] në nivelin e shërbimit të përbashkët. Zhvillimi i përbashkët i liderëve për shekullin 21-të, është produkti i një vazhdimësie të mësimit të përbërë nga trajnime, përvojë stafi dhe operacione, arsim, ushtrime, vetëzhvillim dhe përmirësim. Për të arritur mbizotërimin intelektual kundër kundërshtarëve, duhet të prodhojmë oficerë më të aftë, më të ushtruar dhe më kritikë. Atributet e liderit të dëshiruar dhe udhëheqësit në këtë drejtim. Më poshtë është vizioni për stadet e fundit të vazhdimësisë së edukimit/mësimit të përmirësuar për AUP dhe menaxhimin e talenteve.

---

[1] https://sq.wikipedia .org/ Edukimi holistik - Wikipedia.

Stadet e fundit të detyrueshme të AUP.

Programet AUP duhet t’i sigurojnë studentëve njohuritë dhe aftësitë fillestare për t’i përgatitur ata për shërbim si drejtues luftarakë të përbashkët, oficerë, si stafi më të lartë të elitës ushtarake, që:

- perceptojnë dimensionet ushtarake të një sfide që prek interesin kombëtar, çështjet në nivelin e politikës dhe të rekomandojnë opsione ushtarake të qëndrueshme brenda strukturave mbizotëruese të operacioneve kombëtare dhe ato globalisht të integruara;
- parashikojnë dhe udhëheqin adaptimin dhe inovacionin e shpejtë gjatë një periudhe dinamike të përshpejtimit në shkallën e ndryshimit në luftë nën kushtet e konkurrencës të fuqisë dhe teknologjisë;
- kryejnë luftë të përbashkët, në nivelet operative dhe strategjike, si në të gjitha hapësirat, pjesëmarrje në luftë globale të integruar, duke përfshirë aftësinë për të integruar kontributet tona me ato të aleatëve dhe partnerëve; dhe
- janë drejtues që mendojnë strategjikisht ose elitë në mënyrën se si janë të aftë për të aplikuar dhe që mund të ekzekutojnë dhe të adaptojnë strategjinë përmes fushatave dhe operacioneve. Të gjithë absolventët[2] duhet të posedojnë aftësitë e mendimit kritik dhe krijues, inteligjencën emocionale dhe aftësitë efektive të komunikimit të shkruar, të folur dhe të vizualizuar për të mbështetur zhvillimin dhe implementimin e strategjive dhe operacioneve komplekse.

Programi/kurrikula arsimore duhet rivlerësuar për t’iu përshtatur e përgjigjur sfidave që shtron Strategjia e Sigurisë Kombëtare me ndryshimet përkatëse, ky program i kohës nuk është një rastësi, as nuk vjen lirë; ai duhet të vijë si rezultat i një dizajni me ndryshimet e ndodhura dhe të parashikuara në të ardhmen, i integruar me fakultetet më të mira të vendit tonë dhe vendeve të Aleancës. Zhvillimi i mëtejshëm dhe menaxhimi i Fakultetit të Mbrojtjes dhe Sigurisë në sistemin e AUP kërkon kujdes më të shtuar.

Ne duhet të inkurajojmë oficerët e duhur të ndjekin detyrimet e fakultetit dhe shërbimet të lehtësojnë këto detyrime. Kështu, shërbimet duhet të zbatojnë një gamë të plotë të programeve të menaxhimit të talenteve për të inkurajuar detyrimet e fakultetit. Një detyrim fakulteti duhet të jetë konkurrues, të përmirësojë karrierën, të theksohet gjatë bordit të promovimeve dhe të ndiqet për të siguruar që detyrimet e mëtejshme të përfitojnë nga aftësitë e fituara. Një ndryshim kulturor i këtij procesi kërkon që drejtuesit, në të gjitha nivelet, të vlerësojnë në mënyrë kooperative detyrimet e fakultetit, të eliminojnë pengesat që bllokojnë progresin, dhe të hiqet çdo stigmë që zvogëlon rëndësinë e edukimit të liderëve të ardhshëm. Në këtë mënyrë, duhet të marrim në konsideratë kreditet e përbashkëta për detyrimet e fakultetit në programet e akredituara të AUP, duke lejuar dhe programet tona të dominojnë në disa pozita si të përbashkët.

---

[2] https://sq.wikipedia.org/wiki/Absolventi.

Ne duhet të shpërblejmë talentet me forma e metoda të ndryshme; tërheqim, zhvillojmë dhe mbajmë fakultetin profesional të lartë (FMS) cilësor në institucionet tona të edukimit/mësimit ushtarak; dhe të bashkëpunojmë me fakultetet profesionale civile me akreditimet për të mësuar në nivelet e kërkuara. Për shkak se kurrikulat e AUP duhet të jenë dinamike si mjedis, fakulteti duhet të jetë plotësisht i gatshëm për mësimin praktik, hulumtimin dhe dizajnin e kursit, dhe për vlerësimin, përmirësimin dhe integrimin e vazhdueshëm të kurrikulës. Suksesi gjithashtu kërkon që të investojmë plotësisht në arkitekturën tonë akademike të mbështetjes. Përveç objekteve tona, duhet të sigurojmë burime, të mbajmë dhe të mbrojmë funksionet e rëndësishme të mbështetjes akademike, përfshirë teknologjinë e edukimit dhe informacionit dhe aktivitetet organizative të nevojshme për të fuqizuar fakultetin dhe për të mundësuar studentët të arrijnë rezultatet e kërkuara me përgjegjësitë që duhet të arrijë.

3.4. Të konsiderojmë AUP si një pasuri strategjike[3].

Ne duhet të përdorim programet dhe kurrikulat e AUP-së si një pasuri strategjike për të ndërtuar besim dhe operacionalitet në të gjithë Forcën e Armatosur dhe për t’u integruar me aleatët dhe partnerët ndërkombëtarë. Për të përparuar në këtë element:

- Institucionet tona të AUP-së duhet të jenë një strukturë fleksibël dhe të prirur për adaptim. Bashkëpunimi në rrjetin tonë AUP përmirëson programet tona, ndërton sinergji dhe kuptim më të thellë, dhe na lejon të përqendrohemi në problemet kyçe. Në proces, enti i edukimit mund të shërbejë studentëve/kursantëve ushtarakë me studime dhe hulumtime rigorozë, zhvillim konceptesh dhe dizajnimin e ushtrimeve. AUP duhet të jetë dinamik. Për të mbetur relevante, duhet të vlerësojmë periodikisht programet tona, të validojmë misionet dhe fokuset, si dhe të përcaktojmë boshllëqet dhe nevojën për programe të reja. Në të njëjtin kohë, duhet të përpiqemi për të bërë entin tonë AUP të qasshëm për Forcën tonë të Armatosur dhe të mbështesim programet e zhvillimit vetjake dhe të zhvillimit profesional të Forcave e njësive, duke njohur që këto t'i përgjigjen misionit bazë.

---

[3] https://www.jcs.mil/doctrine/.

- Ne duhet të vazhdojmë të përfshijmë dhe shkëmbejmë eksperienca në studime brenda sistemit tonë AUP dhe sistemet arsimore ushtarake jashtë vendit, studentët tanë dhe ato aleatë dhe partnerë, për të përgatitur më mirë oficerët tanë për operacione të përbashkëta. Marrëdhëniet e forta mes institucioneve AUP janë gjithashtu të rëndësishme për tu integruar në programet e AUP të vendeve të tjera aleate në mënyrë që ne të zhvillohemi, duke krijuar mundësi për lidhje më të ngushta dhe bashkëpunim më të thellë, si dhe për pjesëmarrje më të madhe të studentëve tanë.

- Ne duhet të përfshijmë si Forcën e Armatosur ashtu edhe civilë të Ministrisë së Mbrojtjes dhe dikastere të tjera të vendit dhe vendeve aleate në programet e zhvillimit në nivelin më të lartë të AUP për të siguruar që ata të kontribuojnë në të ardhmen. Gjithashtu, duhet të forcojmë perspektivat tona me institucionet e tjera të vendit tonë dhe ato partnere.

3.5. Të rregullojmë edukimin dhe përdorimin e talentit.

Përdorimi me qëllim i të diplomuarve të AUP është një detyrë themelore që lidhet drejtpërdrejt me rezultatet më të mira të procesit. Sot kërkohen procese efektive për caktimin dhe përdorimin e personelit të diplomuar në AUP për të siguruar që në detyrat e marra gjatë karrierës të përfitojnë nga arritjet akademike dhe edukimi i marrë. Ne duhet të përdorim me qëllim përvojën akademike, hulumtimin dhe mësimin eksperimental të të diplomuarve të AUP-së në një shkallë më të madhe. Duhet të sigurojmë që vlerësimet akademike të kapin arritjet dhe ekspertizën e oficerëve për të ndihmuar proceset e menaxhimit të talenteve. Për të arritur vizionin e përcaktuar këtu, duhet të shpërblejmë oficerët ekselent me detyra të përshtatshme dhe potencialin për të mbetur konkurrues në karrierën e tyre. Gjithashtu, duhet të sigurohemi që po prodhojmë një numër të mjaftueshëm oficerësh të kualifikuar të përbashkët në sistemin tonë AUP për stafet e strukturave të FA dhe ato të përbashkëta.

3.6. Të përdorim ushtrime të përbashkëta.

Përdorimi i ushtrimeve gjithashtu është një pjesë kyçe e vazhdimësisë të edukimit ushtarak. Ne duhet të jemi të gatshëm të vendosim pjesëmarrësit në ushtrime në situata të paqartësisë dhe kompleksitetit, ku krijimi, adaptimi, mendimi kritik dhe iniciativa janë theksuar dhe treguar. Planifikimi dhe zbatimi i aftësive të avancuara duhet të jetë një pjesë kyçe e këtyre ushtrimeve për të përforcuar kapacitetet në zhvillim, për të njohur problemet dhe mundësitë dhe për të nisur marrjen e vendimeve të shpejta si një aspekt themelor i operacioneve të integruara të përbashkëta. Ushtrimet tona të përbashkëta duhet të përdoren si një mekanizëm rregullator që lidh çështjet dhe edukimin në zhvillimin tonë të udhëheqjes dhe sistemin tonë AUP. Në anën tjetër, studiuesit/kërkuesit dhe pedagogët tanë në AUP mund të kontribuojnë me studimet e tyre edukative për të mbështetur gjithashtu drejtuesit ushtarak.

3.7. Të identifikojmë dhe zhvillojmë elitë ushtarake.

Ne kemi nevojë për një grup të zgjedhur oficerësh që mund të kontribuojnë në mënyrë të kuptueshme në formulimin e strategjive. Vendi (Forcat e Armatosura) ka nevojë për procese për të identifikuar dhe zhvilluar elitë, jo vetëm planifikues operacionale dhe fushatë, por edhe shkollat AUP dhe oficerët gjenerues, duhet të luajnë një rol aktive në identifikimin e talenteve elitë dhe inovatorë. Shkollimi civil i avancuar, bursat dhe mundësitë për zgjerim ofrojnë një përmirësim të vlefshëm për sistemin tonë AUP, por duhet të kenë rezultate të qarta dhe nuk kualifikohen si pjesëmarrës në AUP. Një numër i zgjedhur i studentëve në programet tona AUP do të tregojnë potencialin për të qenë më shumë se elitë ushtarake; ata gjithashtu do të kenë aftësi për të dizajnuar kreativitet, strategji politiko-ushtarake të integruara ose për të zhvilluar koncepte doktrinare të reja.

Si rrjedhojë, duhet të krijojmë dhe të ruajmë mundësi në kurrikulat tona për specializim. Ne duhet të identifikojmë këtë elitë ushtarake dhe të përshtatim programe për ta zhvilluar mendimin dhe kontributet e tyre.

Përfundime

Sot, ballafaqohemi me një të ardhme që kërkon ndryshime tërësore nga e sotmja, për të arritur rezultatet e pritshme të së nesërmes, për këtë ne duhet të identifikojmë dhe të zgjedhim oficerët që tregojnë përparësi intelektuale dhe që mund të zgjidhin situata përpara kundërshtarëve tanë në luftë mes pasigurisë dhe ndryshimeve të sotme. Krijimi i superioritetit intelektual dhe gatishmëria mendore që ne kërkojmë nuk mund të arrihet me edukim sporadik ose vetëm me përvojë të mëparshme. Ai krijohet nga kombinimi i edukimit, trajnimit, ushtrimeve rigoroze dhe zbatimit në botën reale. Për të përmbushur këtë objektiv, duhet një rrugë e përhershme e transformimit që duhet të filluar. Kërkohen përpjekje të përbashkët në të gjithë FA, për të vendosur bazat për të zbatuar këtë vizion. Rezultati do të jetë një ndryshim kulturor dhe intelektual në FA. Një investim në aspektet njohëse të profesionit tonë nuk është i mjaftueshëm. Ne duhet të sigurojmë që të zhvillojmë mekanizma që integrojnë programet e AUP dhe menaxhimin e talenteve, duke vlerësuar dhe përmirësuar vazhdimisht, duke lëvizur zhvillimin e drejtueseve ushtarak në rrugën tonë më të arrirë, pra AUP, për të adresuar me krijimtarinë nevojat tona më të rëndësishme luftarake.

Bibliografia

1. Strategjia e Sigurisë Kombëtare e RSH 14/2024.
2. Strategjia Ushtarake 2024.
3. Intellectual preparation for future war, by; Mick Ryan.
4. Arsimimi dhe Stërvitja në Forcat e Armatosura Dhjetor 2015.
5. Koncepti i arsimimit dhe trajnimit individual të personelit të Forcave të Armatosura të Republikës së Shqipërisë.
6. https://www.jcs.mil/doctrine/.

Realiteti virtual dhe përfitimi i tij në Forcat e Armatosura

Kryekapter Gëzim Mataj
Nënoficer në Regjimentin e Operacioneve Speciale

Trajtesë e shkurtuar.

Realiteti virtual (RV), po shfaqet me shpejtësi si një fushë e re e kërkimit multidisiplinor. Gjatë dy viteve të fundit, qëllimi i tij është rritur përtej kërkimit akademik dhe industria është gjetur duke bërë investime të rëndësishme në këtë fushë si për kërkimin, ashtu edhe për prodhimin e zhvillimit të produkteve të ndryshme të bazuara në RV. Sektorë të ndryshëm industrialë si teknologjia e informacionit, inxhinieria biomjekësore, sektori i teknologjisë së projektimit strukturor dhe ndihmës trajnimi po investojnë në këtë teknologji. Industria ushtarake e cila mbetet gjithmonë në kërkim të ideve të reja po shfaqet ngadalë si një nga investitorët kryesorë në RV. Ky shkrim paraqet një vlerësim rreth rëndësisë së RV për Forcat e Armatosura të RSH.

Fjalë kyçe*:* Realiteti virtual (RV), bota reale, simulatorët e botës virtuale, luftë, ushtri.

Hyrje

Realiteti virtual (RV) është një nocion shekullor. Por, në vitet e kaluara nuk ishte artikuluar në mënyrën se si bëhet në kohën e sotme. Shumë breza më parë, filozofi grek Platoni (427-347 p.e.s.) u kishte ofruar sundimtarëve të atëhershëm një perspektivë në lidhje me vendimmarrjen politike. Ai u kishte kërkuar atyre që vendimet politike t'i merrnin në mënyrë rigoroze në bazë të njohurive të caktuara dhe jo në bazë të intuitës. Për të shpjeguar argumentin e tij, ai kishte paraqitur një metaforë në formën e "të burgosurve të bllokuar në shpellë”. Ky formulim paraqet një pikëpamje se njerëzit që kanë kaluar jetën e tyre në shpellë të lidhur me zinxhirë, fillojnë t’i besojnë si të vërteta “hijet” që i shohin në errësirë. Platoni donte që klasa politike të ndante hijet nga substanca. Ndoshta, Platoni mund të shihej se po parashtronte konceptin analog me realitetin virtual në ato kohë. Mund të jetë e diskutueshme nëse ai e shpalli apo hoqi dorë nga koncepti i realitetit virtual; megjithatë, ai ishte padyshim instrumental në nxjerrjen në pah të manifestimit të dukshëm të realitetit “alternativ”. Me kalimin e viteve, koncepti i realitetit virtual ka evoluar ndjeshëm. Në veçanti, zhvillimet e rëndësishme që po ndodhin në fushën e sektorit të teknologjisë së informacionit kanë revolucionarizuar ndjeshëm terrenin e realitetit virtual. Aktualisht, aplikacionet e realitetit virtual po gjejnë shërbime në fusha të ndryshme të jetës, nga shkencat kompjuterike në inxhinierinë mekanike, tek inxhinieria biomjekësore, te mjekësia dhe arkitektura. Forcat e armatosura gjithashtu po identifikojnë aplikacione të ndryshme të bazuara në RV, për përdorimin e tyre. Duket se kjo teknologji ka të ngjarë të gjejë më shumë dobi për forcat e armatosura në vitet në vijim. Ky punim tenton të analizojë efikasitetin e kësaj teknologjie për arkitekturat e sigurisë të shteteve.

1. Ideja e realitetit virtual

Ashtu si shumë zbulime të tjera shkencore, realiteti virtual i ka rrënjët në romanet dhe esetë fantastike-shkencore. Përvoja e parë e RV, mund të thuhet se erdhi në vitin 1962, me krijimin e makinës së quajtur “Sensorama” e cila në thelb ishte lojë duke i dhënë lojtarit një përvojë të ngasjes së një motoçiklete në rrugë.

Kjo u zhvillua nga Morton Heilig i cili me profesion ishte kinematografik. Qëllimi i tij ishte të bashkonte të pesë shqisat në një përvojë virtuale. Që atëherë, realiteti virtual e ka bërë të ndjehet prania e saj kryesisht në arenën e argëtimit, veçanërisht për zhvillimin e lojërave video dhe filmave. Aktualisht, fusha e RV po rritet shumë përtej industrisë së argëtimit dhe mbulon një spektër të gjerë idesh në fushën e përgjithshme të teknologjisë. Ndoshta, natyra përfshirëse e kësaj teknologjie po e bën të vështirë përcaktimin e realitetit në terma të saktë.

Është e vështirë të gjesh përkufizimin standard për RV në literaturë. Sidoqoftë, duket se ka një kuptim të përbashkët për atë që ka të bëjë realiteti virtual, e ndryshme gjendet vetëm në semantikë nga autori në autor. Termi RV u krijua nga Jaron Lanier, themeluesi i VPL (Virtual Programming Language) Research në SHBA, një nga shtëpitë origjinale të biznesit që shet sisteme të RV. Termi u përkufizua si “një mjedis i krijuar nga kompjuteri, interaktiv, tredimensional në të cilin një person është i zhytur (Aukstakalnis dhe Blatner 1992)”. Në mënyrë të thjeshtë, RV është një mjedis artificial i krijuar duke përdorur mjete të teknologjisë së informacionit (si Harduer ashtu edhe Softuer) dhe i paraqitet përdoruesit në atë mënyrë që të duket dhe të ndihet si çdo mjedis real. Është e rëndësishme të theksohet se bota virtuale është ndërvepruese, gjë që e bën përdoruesin të zhytet plotësisht në një botë artificiale larg mjedisit real. Për të përjetuar RV, individi duhet të përdorë dy nga pesë shqisat e tij: shikimin dhe zërin. Për të përjetuar/ndjerë kryesisht imazhet tredimensionale, përdoren pajisje të tilla si modulatorët e frekuencës, mausi, leva, kufjet, dorezat speciale, ekrani i montuar në kokë dhe syzet. Të gjitha këto pajisje punojnë në hyrje nga një sistem kompjuterik. Është e rëndësishme të theksohet se kryesisht nuk është e mundur të krijohet një kopje e saktë e botës reale. Gjithmonë do të kishte një lloj ndryshimi midis botës reale dhe asaj virtuale. Prandaj, ekzistojnë dallime thelbësore midis botës reale dhe asaj virtuale. Një punë e cila në fakt është e thjeshtë rezulton të jetë shumë e vështirë në një mjedis të RV si nga pikëpamja e projektimit ashtu edhe nga ana e ekzekutimit.

Një veprim i thjeshtë i mbajtjes së topit në dy duar është shumë i ndërlikuar në botën virtuale. Në realitet, një top mbahet, i mbajtur me dy duar, pozicioni i duarve përcaktohet nga sipërfaqja e topit dhe kontrolli i topit sigurohet nga haptika (haptika = prekja = lidhja) dhe shqisat vizuale të njeriut. Në një mjedis virtual, ku nuk sigurohet reagime haptike, kontrolli i topit duhet të kryhet ekskluzivisht nga sistemi vizual.

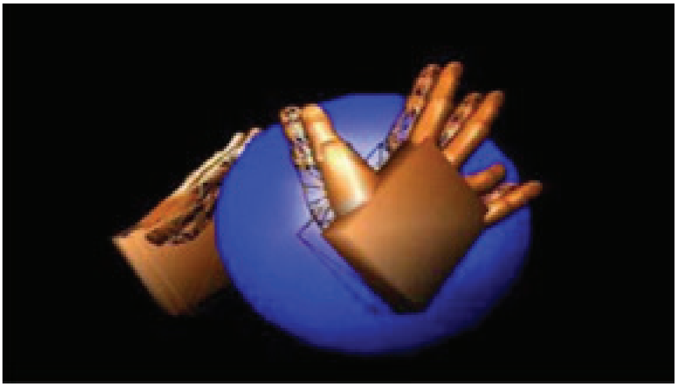


Figura nr. 1.
Mbajtja e një topi me dy duar virtuale; duart opake tregojnë pozicionet e duarve virtuale, duart me kornizë teli tregojnë pozicionet e duarve reale të përdoruesit. Ato, ndryshe nga duart virtuale, janë në gjendje të depërtojnë në top.

Ka disa aspekte që e bëjnë shumë më të vështirë kontrollin e topit në mjedisin virtual sesa në realitet. Prandaj, përdoruesi duhet të trajnohet për të punuar në një atmosferë në të cilën ai/ajo nuk po mban vërtet një top (në fakt ai/ajo nuk mban asgjë), ai/ajo duhet të pozicionojë duart e tij/saj të vërteta sipas lëvizjes vizuale të riprodhimit të duarve të tij. Kjo shkakton një stimulim krejtësisht të ndryshëm të muskujve të përdoruesit sesa me një top të vërtetë (pa peshë dhe pa kundërforca nga topi). Gjithashtu, cilësia e pozicionit të riprodhimit të topit dhe të duarve në shumicën e rasteve nuk është perfektë (Fig. 1).

Industria e argëtimit e cila përdor teknikat e realitetit virtual në mënyrë rutinë po përpiqet të improvizojë konceptin ekzistues të realitetit virtual. Ideja e 4D dhe realitetit virtual, ka rëndësinë e saj më shumë për industrinë e argëtimit. Termi “4D”, tregon të katërtin dimension. Ky koncept nuk ka nevojë të përfshijë domosdoshmërisht ndonjë rol kryesor për Softuerin kompjuterik, por përfshin më shumë efekte fizike. Këtu spektatorët mbajnë syze 3D dhe sipas kërkesës së skenës së veçantë, teatrot janë krijuar për të tundur, spërkatur ujë, për të futur erëra dhe madje edhe për të spërkatur ajrin tek publiku për të gjeneruar efekte të ndryshme. Ka pak ide të tjera në praktikë që fabrikojnë realitetin. Realiteti i shtuar është një ide e tillë që ka të bëjë me pamjen e drejtpërdrejtë ose të tërthortë të një mjedisi fizik të botës reale. Këtu elementët e realitetit të shtuar nga kompjuteri virtual gjeneron të dhëna shqisore si zëri ose grafika. Nëse realiteti virtual është një zhytje e plotë në një botë digjitale, realiteti i shtuar është më shumë një mbivendosje digjitale në botën reale.

Ai e shton botën reale me të dhëna digjitale duke e bërë atë më emocionues sesa një mjedis krejtësisht fiktiv.

Një shembull i realitetit të shtuar mund të jetë dëshmimi i botës përreth nesh, siç shihet përmes kamerës së telefonit tonë, e krahasuar me hyrje të tjera si informacioni i vendit të bazuar në GPS (Schonfeld 2011). Një koncept tjetër shumë i diskutuar në këtë fushë është ai i realitetit të ndërmjetësuar. Këtu pamja e realitetit modifikohet nga një praktikant kompjuteri që përmirëson perceptimin aktual të realitetit. Një nocion tjetër i ngjashëm është një realitet i përzier. Është një lloj realiteti virtual, por një koncept më i gjerë se realiteti i shtuar, i cili shton botën reale me të dhëna elektronike sintetike. Në anën e kundërt, ekziston një term, virtualiteti i shtuar, i cili përmirëson mjedisin virtual me të dhëna nga bota reale. Realiteti i përzier mbulon një vazhdimësi nga realiteti shtuar në virtual i shtuar Tamura et al.(2001). Aktualisht, literatura dhe debatet e ndryshme në vazhdim mbi temën e realitetit virtual, pikëpamjet e shkencëtarëve që punojnë në këtë fushë dhe perceptimet e përgjithshme tregojnë se realiteti virtual përfshin fusha të mëdha dhe nganjëherë të larmishme idesh dhe teknologjish, duke përfshirë si teleoperatorët ashtu edhe sistemet e mjedisit virtual. Në vende të ndryshme, njerëzit përdorin terminologjitë si realiteti virtual, mjedisi virtual, telerobotika, realiteti i shtuar dhe mjediset sintetike në mënyrë sinonike. Është e rëndësishme të theksohet se meqenëse kjo fushë e kërkimit është ende në zhvillim dhe ka një element të qasjes multidisiplinore me raste, çdo ide e re në vend që të bëhet një nëngrup i fushës së realitetit virtual po projektohet si një fushë e re zhvillimi. Mund të jetë në një nivel teorik, një shpërndarje e tillë është thelbësore për të kuptuar më mirë, por nganjëherë në nivel praktik bëhet e ndërlikuar të diskutohet përparimi teknologjik si një entitet më vete, veçanërisht kur ka një mbivendosje idesh në lidhje me kategori të ndryshme. Realiteti virtual është një teknologji që pritet të ketë një zbatim më të gjerë ushtarak dhe një tërheqje universale të sigurisë. Kjo teknologji ka potencialin të ndikojë në të ardhmen e industrisë globale në përgjithësi dhe të industrisë ushtarake në veçanti. Aktualisht, kërkimi dhe zhvillimi në arenën e realitetit virtual është në nivele të ndryshme arritjesh në pjesë të ndryshme të botës. Arritjet e kësaj teknologjie ende nuk janë vërtetuar, por shumë analistë parashikojnë se kjo teknologji mund të sjellë revolucion me përparime të rëndësishme në të ardhmen e afërt.

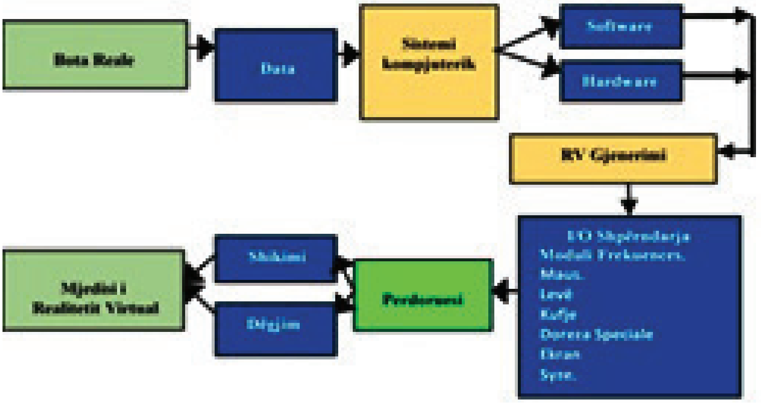


Figura nr. 2. Përshkrim i thjeshtë i konceptit të Realitetit Virtual (RV).

2. Efikasiteti ushtarak IRV

Është një fakt i njohur se teknologjia është jashtëzakonisht e rëndësishme për efektivitetin ushtarak për çdo shtet-komb. Induksioni i teknologjive të reja dhe në zhvillim premton një forcë ushtarake cilësore superiore të aftë për të trajtuar si kërcënimet konvencionale ashtu edhe ato asimetrike. Konceptet ushtarake si revolucioni në çështjet ushtarake kanë natyrë dinamike dhe kanë të bëjnë me futjen e ndryshimeve teknologjike dhe doktrinare në forcat e armatosura. Revolucioni i fundit në sektorin e teknologjisë së informacionit dhe komunikimit ka sjellë induksionin e teknologjive të reja, të revolucionit të çështjeve ushtarake në ushtri. Ushtritë moderne janë gjetur duke induktuar degë të përparimeve të ndryshme në teknologji të tilla si nanoteknologjia, bioteknologjia, robotika, shkencat njohëse dhe pak të tjera në skemën e tyre. Teknologjitë ushtarake gjenden gjithashtu duke përdorur simulime të ndryshme kompjuterike të sistemeve që u mundësojnë atyre të kryejnë operacione në sistemin e simuluar dhe të demonstrojnë efektet në kohë reale.

3. Teknologjia e simulatorit

Trajnimi është një fushë ku teknologjitë RV po gjejnë zbatim më të gjerë në ushtri. Arsyet që e kanë shtyrë ushtrinë të eksplorojë dhe të përdorë teknikat RV në trajnimin e tyre, në thelb janë reduktimi i ekspozimit ndaj rreziqeve dhe rritja e fshehtësisë (Herrero dhe de Antonio 2005). Simulimi i realitetit është thelbësor për ushtarakët për një arsye të thjeshtë se nuk mund të ketë ‘trajnim në punë’ për sa i përket luftës. Nganjëherë, bëhet gjithashtu jashtëzakonisht e vështirë t’i demonstrosh ushtarakëve sfidat e jetës reale mendore dhe fizike të jetës ushtarake. Në rrethana të tilla, lind nevoja për të fshirë realitetin në një formë apo tjetër. Kjo është ajo ku aplikacionet VR të krijuara posaçërisht për ushtrinë mund të luajnë një rol të madh.

Një aspekt i rëndësishëm i simulimit të bazuar në RV është se ai ofron një hapësirë, për të ndërmarrë manovra të ndryshme të rrezikshme dhe të ndërlikuara të cilat janë të vështira për t’u kryer në jetën reale në pajisjet reale. RV bën të mundur simulimin e një mosfunksionimi të pajisjeve ose motit të keq ose ndonjë skenari të papritur (Molloy 2009). E gjithë kjo bëhet e mundur pa shkaktuar asnjë dëm as për njerëzit, as për instrumentet. RV ndihmon për të trajnuar pilotët për të trajtuar emergjencat.

Organizata e Traktatit të Atlantikut të Veriut, në vitin 2003, doli me një raport të rëndësishëm të titulluar “Realiteti Virtual: Gjendja e kërkimeve ushtarake dhe aplikacioneve në vendet anëtare”. Është identifikuar se çelësi i efektivitetit të realitetit virtual për qëllime ushtarake është ndërfaqja njeri-makinë ose ndërveprimi njeri-kompjuter. Personeli ushtarak duhet të jetë në gjendje të kryejë detyrat dhe misionet e tij duke përdorur pajisjet e ekranit ndijor RV dhe pajisjet e reagimit. Këto pajisje duhet të shfaqin një mjedis që ofron sinjalet dhe përgjigjet e duhura të nevojshme për të mësuar dhe kryer detyrat ushtarake. Këtu mund të përmendim disa çështje:

-përcaktimin e aftësive perceptuese dhe kufizimet e pajisjeve të ekranit ndijor;

-projektimin e bazave të të dhënave të terrenit dhe ekraneve të tjera për të përmbushur nevojat e performancës së detyrave;

-të kuptuarit e kompromiseve të performancës njerëzore dhe detyrave të kërkuara nga teknologjitë aktuale;

-vlerësimin e transferimit të trajnimit dhe njohurive nga bota virtuale në atë reale; dhe duke marrë parasysh shkaqet dhe zgjidhjet për sëmundjen e simulatorit që mund të ndodhë në realitetin virtual.

Raporti identifikon aplikacionet bazë ushtarake që përfshijnë RV si sisteme të afta për të ndihmuar në modelimin e sistemeve të armëve dhe për të vlerësuar dhe testuar sisteme të tilla. Gjithashtu, është theksuar se: RV, është e dobishme në zhvillimin e aplikacioneve të trajnimit dhe të të mësuarit dhe mund të luajë një rol për të ndihmuar në planifikimin dhe provën e misionit.[1] Simulatorët e përdorur për trajnimin e fluturimit mund të shihen si një nga përdorimet e hershme të teknologjisë RV.

Gjatë fundit të viteve 1920 dhe 1930, Link Company (Binghamton, Nju Jork) kishte ndërtuar trajnerë fluturimi dhe shumë pilotë ishin trajnuar atje para dhe gjatë Luftës së Dytë Botërore. Në thelb, këta simulatorë u përdorën për të dhënë trajnime mbi aftësitë e fluturimit natën. Me maturimin e teknologjive të televizionit dhe kamerave video, projektuesit e simulatorëve ishin në gjendje të krijonin një pamje të botës së jashtme gjatë viteve 1950.[2] Që atëherë, zhvillime të ndryshme të dobishme teknologjike po e përmirësojnë teknologjinë e simulatorit gjithnjë e më tej. Ardhja e kompjuterit analog elektromekanik solli disa ndryshime në dizajnimin e simulatorit.

Megjithatë, gjatë viteve 1950 dhe fillimit të viteve 1960, kërkesat në lidhje me lëvizjen dhe sistemet vizuale nuk u zgjidhën tërësisht me teknologjinë në dispozicion. Ardhja e informatikës digjitale rriti shanset e simulimit digjital në kohë reale gjatë viteve 1960. Ai gjithashtu përmirësoi fleksibilitetin, përsëritshmërinë e sistemit dhe ndihmoi në sjelljen e standardizimit.[3] Për çdo simulator, kërkesa themelore është që çdo instrument të funksionojë në mënyrë identike me komponentët/pjesët e tyre që përputhen në botën reale. Gjatë dekadave të fundit, revolucioni i madh që po ndodh në teknologjinë e informacionit dhe shkencat e komunikimit lejon sistemet moderne të asistuar nga RV, të ndërlidhin përdoruesin me një kompjuter dhe të ndërmarrin detyra të ndryshme vizuale 3D dhe të kryejnë ndërveprim në kohë reale. Dobia e çdo sistemi RV, vjen nga cilësia e veçorisë së tij kryesore, zhytja. Është kjo aftësi e sistemit RV që lejon përdoruesin të bëhet pjesë e botës së simuluar, e cila është jashtëzakonisht thelbësore për të kapërcyer hendekun midis virtuales dhe asaj reale.

4. Elementi i domosdoshëm i fuqisë ajrore

Roli i VR në fushën ushtarake rritet përtej simulatorit të thjeshtë të fluturimit. Këtu shumë herë, më shumë se një praktikant operon në botën virtuale duke kërkuar një mjedis më të sofistikuar që shpesh quhet mjedis sintetik i avancuara (Wong 2010). Është thelbësore të krijohet simulimi i luftës ajrore me nivele të larta realizmi. Për këtë qëllim, bëhet i nevojshëm integrimi i modeleve kompjuterike, skenarëve të simuluar dhe modeleve të ndryshme të sjelljes, simulatorëve të platformave fluturuese dhe sistemeve të armëve, si dhe sistemeve të tjera thelbësore të luftimit të luftës. Një mjedis i tillë sintetik mund të përbëjë sisteme të pavarura ose një rrjet rrjetesh. Aktualisht, Forcat Ajrore të SHBA-së po investojnë në aftësi të tilla të trajnimit të misionit të shpërndarë (Lok 2001). Në përgjithësi, përdorimi i RV ofron një alternativë për të avancuar stërvitjen taktike të fluturimit, si dhe ndihmon në zhvillimin e doktrinave dhe taktikave. Kjo gjithashtu mundëson vlerësimin e planeve operative. Në vitet në vijim, trajnimi i simuluar ka të ngjarë të marrë më shumë rëndësi për një arsye të thjeshtë se është me kosto efektive dhe shmang humbjen e jetëve njerëzore. Teknologjia VR pritet të zvogëlojë përpjekjet aktuale të fluturimit, të paktën në një masë të caktuar, sepse ajo ofron metodën më kosto-efektive, për trajnimin e pilotëve. Gjithashtu, pakësimi i aktiviteteve aktuale të fluturimit do të luante një rol në menaxhimin e dëmeve në mjedis.

---

[1] Një raport i NATO-s i titulluar “Realiteti virtual”: Gjendja e kërkimeve ushtarake dhe aplikacioneve në vendet anëtare”, RAPORT TEKNIK
RTO 18, St. Joseph Print Group Inc. St. Joseph Print Group Inc. Otava, Ontario, Kanada, 2003.

[2] http://www.hitl.washington.edu/scivw/EVE/II.G.Military.html.

[3] http://homepage.ntlworld.com/bleep/SimHist8.html. Botuar më 28 Korrik 2010.

Përveç forcave ajrore të SHBA, teknika të tilla përdorin edhe forca të tjera ajrore. Ata kanë zhvilluar koncepte që përdorin mjedisin virtual të ajrit. Forcat ajrore Mbretërore Australiane së bashku me shkencën e tyre të mbrojtjes dhe teknologjisë, ka zhvilluar konceptin simulimit të avancuar. Konceptet e ndryshme të zhvilluara që përfshijnë RV dhe teknikat shoqëruese të simulimit, janë vënë në përdorim për trajnimin operacional nga RAAF veçanërisht nga grupet e tyre të mbikëqyrjes dhe kontrollit (Jon Blacklock dhe Zalcman 2003). Qendrat simulatorë janë krijuar gjithashtu nga Forcat Ajrore Franceze dhe Gjermane. Gjithashtu, projekti Eurofighter nga katër kombet kanë krijuar Ndihmën Trajnuese Sintetike të Eurofighter Aircrew (ASTA).[4]

Ky sistem është vlerësuar si një nga sistemet më të mira në Evropë duke ofruar trajnime të avantazhit, besnikëri të lartë dhe 360^0 fusha të shikimit. Gjatë prillit 2009, simulatori i parë ASTA për Eurofighter Typhoon u bë funksional për Forcën Ajrore Italiane.[5]

Për forcat e tjera ajrore si Forca Ajrore izraelite dhe në shtete si Holanda, sistemet janë vendosur për aktivitete të tilla trajnimi (Lok 2001). Trajnimi i simulatorëve nuk ka mbetur i kufizuar në trajnimin me avionët e transportit luftarak, por gjithashtu mbulon zona si makinat fluturuese pa pilot, p.sh., u krijua një skuadron e re e forcave ajrore izraelite, e dedikuar për ofrimin e trajnimeve të bazuara në simulime për pilotët e helikopterëve dhe operatorët e automjeteve ajrore pa pilot. operacionale gjatë vitit 2010.[6]

---

[4] Për më shumë detaje, ju lutemi vizitoni http://www.eurofighter.com/media/ news0/news-detail/article/aircrew synthetic-training-aids-asta.html dhe http://www.eurofighter.com/media/ news0/news-detail/article/ training-days.html. Botuar më 23 dhjetor 2010.

[5] http://www.eurofighter.com/media/news0/news-detail/article/the first-asta-simulator-for-the-Eurofighter-Typhoon-Operational.html. Botuar më 04 tetor 2010.

Industria e mbrojtjes po përdor teknologjinë RV edhe për qëllime prodhimi. Sikorsky Aircraft Corp. një degë e United Technologies Corp. gjatë janarit 2011, zbuloi një qendër moderne të realitetit virtual për programin e helikopterëve të ngritjes së rëndë CH-53K. Ky mjet inovativ ndihmon në identifikimin e boshllëqeve në një mjedis digjital tredimensional përpara montimit eksperimental. Kjo lejon kursime të kostos dhe efikasitet më të madh dhe ndihmon në minimizimin e vonesave në montimin përfundimtar të avionit. Qëllimi është të përmirësojë aftësinë e projektuesit për të projektuar një avion që është më i lehtë për t'u mirëmbajtur.[7]

Kryesisht, midis vendeve në zhvillim, shumica e të cilave nuk kanë industrinë e tyre të avionëve, trajnimi i simulatorëve jepet nga prodhuesit e pajisjeve origjinale (OEM). Shtetet si Kina kanë zhvilluar infrastrukturën e tyre të simulatorëve. Në Kinë, puna e kërkimit dhe zhvillimit në lidhje me RV filloi në fillim të viteve 1990. Aktualisht, universitete të ndryshme dhe institucione shkencore janë përfshirë në zhvillimin e kësaj teknologjie. Në fushën e mbrojtjes, puna është ndërmarrë në Universitetin Kombëtar të Teknologjia e Mbrojtjes. Këtu teknologët ushtarakë po punojnë në projekte duke përfshirë realitetin virtual të shpërndarë, modelimin e sjelljes, mjetet e modelimit dhe paraqitjes së bazuar në imazh (IBMR), simulimin e valëve dinamike të oqeanit dhe zbulimin e përplasjeve (Pan et al. 2000). Sipas ekspertëve, shërbimet e ushtrisë kineze (PLA) përdorin një sërë simulatorësh për një sërë objektivash trajnimi. Ata bëjnë simulatorët e tyre individualë ose të ekuipazhit për raketat balistike dhe ato të lundrimit, luftëtarët e gjeneratës së 4-të, trajnerët, nëndetëset, anijet, tanket kryesore të betejës, automjetet e tjera të blinduara, kamionët, raketat me rreze të gjatë dhe të lëshuar me shpatull (SAM), të shtënat dhe trajnime individuale për vendime luftarake.

Megjithatë, nuk dihet shumë për densitetin e shpërndarjes së simulatorit. Pritet që PLA do të rrjetëzojë simulatorë të ndryshëm për të mundësuar simulimin e misionit të nivelit komandues dhe të nivelit luftarak individual, madje mund të jetë simulim i përbashkët i forcës në prag të misioneve aktuale.[8] Veçanërisht, për mësimin e detyrave të ndërlikuara si fluturimi është shumë e rëndësishme të zhvilloni ndjenjën e pranisë në mjetet ndihmëse të trajnimit për ta bërë përvojën e të mësuarit tërheqëse dhe relevante.

---

[6] http://www.flightglobal.com/articles/2010/10/04/348060/israelopens-helicopter-uav-imulator -unit.html. Botuar më 20 Tetor 2010.

[7] http://www.defencetalk.com/sikorsky-virtual-reality-for-ch-53khelicopter-31398/#ixzz1ECGOf1TH. Botuar më 12 Janar 2011.

[8] Në bisedë me Richard D Fisher Jr., një ekspert me bazë në SHBA për Kinën dhe autor i librit *Modernizimi Ushtarak i Kinës* (Praeger Security International, Londër, 2008).

Është e rëndësishme që të trajnuarit të përjetojnë mendime, emocione dhe sjellje të ngjashme me ato që mund të përjetojnë në një situatë të jetës reale. Ndjenja e pranisë në situatën e stërvitjes ndihmon gjithashtu në analizimin e problemeve pas stërvitjes.[9] Për të përmirësuar trajnimin për kontrollorët dhe vëzhguesit e zjarrit me qëllim të koordinimit të sulmeve ajrore për operacionet luftarake të mbështetjes së ngushtë ajrore, teknikat RV kanë dobi të konsiderueshme. Gjithashtu, sistemet e simulatorëve të bazuara në RV ofrojnë një video me imazhe foto-realiste të zonës aktuale të shtrirjes së mbivendosur në të dhënat e lartësisë së terrenit me përmirësime tredimensionale të ndërtesave dhe vegjetacionit. Piloti virtual merr aftësinë për të identifikuar trupat dhe automjetet në terren duke përdorur sensorë në bord.[10]

5. Aplikacionet detare

Përveç aviacionit RV përdoret gjithashtu, për prodhimin e simulatorëve për mjetet tokësore dhe automjetet që operojnë në ujë. Simulatorë të tillë hyjnë në kategori të ndryshme nga një automjet i vetëm në një sistem që lehtëson misione komplekse trajnimi që përfshijnë pjesëmarrës të shumtë që veprojnë në role të ndryshme. Pajisjet specifike janë të disponueshme për ushtrinë, të cilat trajnojnë ushtarët për të drejtuar automjete të specializuara si tanke ose shumë mjet i blinduar. Është gjithashtu e mundur të kryhet trajnimi duke përsëritur kushtet e vështirë dhe të pabesa të motit, duke përfshirë mjedisin luftarak urban. Gjithashtu, simulatorët në rrjet janë krijuar për të lejuar përdoruesit të marrin pjesë në lojëra komplekse luftarake.

Kërkesat teknike për simulatorët për Marinën janë paksa të ndryshme. Për simulatorët nënujorë, nuk ka nevojë të ketë dritare drejt botës së jashtme dhe për këtë arsye kërkesa realiste e “mjedisit” dhe “terrenit” nuk ka shumë rëndësi. Ajo që është e rëndësishme është të sigurohen lexime realiste të instrumenteve ndërsa ekuipazhi lundron nëpër simulim. Megjithatë, është gjithashtu e rëndësishme të krijohet një ndjenjë e zhytjes sa më shumë që të jetë e mundur duke simuluar fizikisht një manovër zhytjeje ose daljeje në sipërfaqe (Strickland 2011). Kërkimi dhe shpëtimi (SAR) është një element i rëndësishëm i çdo sistemi të menaxhimit të fatkeqësive të anijeve. Trajnimi i specializuar është i domosdoshëm për personin përpara se të punësohet në departamentin SAR.

RV, ka një dobi në lidhje me trajnimin për qëllime të tilla. Sisteme të tilla janë sisteme simulimi të sintetizuara dhe ato integrojnë simulatorë të ndryshëm së bashku si: imitues i trajtimit të anijeve, simulator i dhomës së motorit, etj. Sistemi krijon një mjedis virtual me efekt të fortë zhytjeje dhe siguron një sistem simulimi realist me realizëm më të mirë mjedisor, realizëm fizik, dhe realizmi i sjelljes (Yin et al. 2010).

---

[9] Për më shumë rreth kësaj, ju lutemi referojuni Ch11 nga Fabrizia Mantovani dhe Gianluca Castelnuovo, “Ndjenja e prezencës në trajnimin virtual: Përmirësimi i përvetësimit të aftësive dhe transferimi i njohurive përmes përvojës mësimore në mjedise virtuale” në riva et al. (2003).

[10] http://www.usafe.af.mil/news/story_print.asp?id=123168023. Botuar më 12 janar 2011.

6. Projektimi inxhinierik

Përveç trajnimit simulator, RV dhe degët e tij aleate kanë dobi në fusha të tjera të ndryshme të lidhura drejtpërdrejt ose tërthorazi me forcat e armatosura. Projektimi inxhinierik është një fushë e tillë. Zbatueshmeria e RV mund të jetë e gjerë, duke filluar nga industria e mbrojtjes deri tek punëtoritë e nivelit lokal në institucione të ndryshme ushtarake. RV mund të ndihmojë procesin e zhvillimit të prototipeve për pajisje të ndryshme. Realiteti virtual dhe realiteti shtuar ka një zbatim më të gjerë në lidhje me prodhimin, mirëmbajtjen dhe riparimin e pajisjeve të ndryshme ushtarake. Për adresimin e çështjeve që lidhen me pajisje të reja ose të panjohura, në vend që të hapni disa manuale riparimi, thjesht një ekran i realitetit të shtuar mund të jetë i dobishëm. Sistemet VR kanë provuar dobinë e tyre për dizajnet e konsumatorëve.[11]

Interesi në rritje i ushtrisë në teknologjinë e realitetit virtual është kryesisht nga perspektiva e kostos dhe sigurisë. Është me kosto efektive testimi i modeleve konceptuale në lidhje me sistemet e armëve ose platformat e mirëmbajtjes duke përdorur teknologjinë RV.[12] Teknologjia lejon testimin e dizajnit pa ndërtuar një prototip fizik. Kjo kursen kohë me në lidhje me zhvillimin e teknologjisë. Vizualizimi i fushëbetejës është një fushë tjetër ku RV ndihmon në përmirësimin e sistemeve të ushtrisë. Vizualizimi i fushëbetejës nuk është vetëm një element kyç në regjimin e stërvitjes, por është gjithashtu jetik për përcaktimin e strategjive luftarake në kohë reale. Për sistemet RV, tani është e mundur që zyrtarët ushtarakë të eksplorojnë një model tredimensional të një zone duke e parë atë nga çdo kënd, ndërsa formulojnë strategji dhe kërkojnë probleme të mundshme logjistike (Strickland 2010)

7. Zbatueshmeria mjekësore

RV ka një zbatim të madh edhe në fushën e mjekësisë, veçanërisht në arenat e kirurgjisë së drejtuar nga imazhi. Teknikat RV po bëhen më tërheqëse në shkencën moderne mjekësore. Teknikat si tomografia e kompjuterizuar dhe skanimet e rezonancës magnetike imazherike (CT/RMI) mund të shihen si teknikat më të përdorura të teknologjisë VR në mjekësi. Një skanim MRI krijon imazhet e një strukture trupi bazuar në një teknikë duke përdorur fushën magnetike. Kjo teknikë është jashtëzakonisht e dobishme për qëllimet e diktimit të sëmundjes. Një tomografi aksiale e kompjuterizuar e njohur zakonisht si skanim CT/CAT përdor imazhe të shumta me rreze X për të krijuar një pamje tërthore/tredimensionale të pjesës së trupit dhe ndihmon në diktimin e sëmundjes.

---

[11] http://www.se.rit.edu/*jrv/research/ar/introduction.html. Akses më 10 shkurt 2011.

[12] http://www.designnews.com/article/7775-Military_Broadens_Use_of_Virtual_Reality.ph

Për shumë vite, teknika e rrezeve-X, ka qenë komponenti kryesor i imazhit mjekësor. Ardhja e kompjuterit ka sjellë një revolucion në fushën e imazheve mjekësore. Një faktor kyç në përparimet në kirurgjinë e udhëhequr nga imazhi (IGS) është aftësia jo vetëm për të regjistruar imazhe që rrjedhin nga modalitetet e ndryshme të imazhit ndërmjet tyre, por edhe për t'i regjistruar ato te pacienti. Aspekti tjetër thelbësor i IGS është aftësia për të gjurmuar instrumentet në kohë reale gjatë procedurës dhe për t'i portretizuar ato si pjesë e një modeli realist të vëllimit operativ. Teknikat stereoskopike dhe të realitetit virtual mund të përmirësojnë në mënyrë të dobishme procesin e vizualizimit (Peters 2000). Teknika të tilla kanë dobi të madhe edhe në aplikimet kurrizore dhe ortopedike. Nga pikëpamja e forcave të armatosura ku energjia është kryesisht kritike dhe e ndryshme nga aksidentet e zakonshme (lëndimet dhe dëmtimet në fushëbetejë afër trupit të njeriut janë të ndryshme nga rastet normale), teknika të tilla janë shumë të dobishme.

Teknologjia haptike po gjen gjithnjë e më shumë dobi në fushën e mjekimit. Kjo teknologji përdor ndërfaqet me kompjuterët për të prodhuar ndjenjën e prekjes duke aplikuar forca të ndryshme. "Këto forca mund t'i bëjnë imazhet/realitetin virtual të duken realë në prekje. Ndërfaqet lejojnë që disa trupa të prekin, ndjejnë, stimulojnë dhe ndryshojnë dimensionet objekte në sferën virtuale. Telerobotika është një zonë e madhe që përdor sisteme haptike. Telekirurgjia është kur një kirurg nuk është i pranishëm në dhomë dhe mund ta bëjë operacionin nga sfera virtuale (Boduch 2010)". Përdorimet e teknikave RV për mjekësi kanë dobi të mëdha për spitalet si në domenin civil ashtu edhe atë ushtarak. Veçanërisht, teknikat si Telekirurgjia, mund të jenë të dobishme në rastin e bazave përpara për forcat e armatosura ku janë të disponueshme lehtësira minimale mjekësore.

Teknologjia RV gjithashtu ka dobi, për një sërë ndërhyrjesh psikosociale. Vitet e fundit, një numër në rritje i terapistëve profesionistë kanë integruar teknologjitë e teknologjisë së lojërave video në programet e rehabilitimit. Ato janë përdorur me sukses në rritjen e motivimit të pacientëve dhe inkurajimin e lëvizjes së plotë të trupit. Për të bërë sisteme që janë më miqësore me pacientët, janë projektuar pak sisteme me kosto të ulët, të bazuar në VR, të cilat përdorin elemente dëgjimore, vizuale dhe haptike për të ofruar reagime dhe motivim të jashtëm për pacientët (Anderson et al. 2011). Komuniteti mjekësor i Forcave të Armatosura duhet të trajtojë shumë pacientë me rehabilitim fizik dhe përdorimi i teknikave të bazuara në VR i ndihmon ata jo vetëm të ndihmojnë pacientët, por edhe të përmirësojnë moralin e trupave. Ushtarakët gjenden duke përdorur teknologjinë RV përtej praktikave rutinë mjekësore. Ata janë gjetur duke përdorur botën virtuale për të trajtuar veteranët e traumatizuar të luftës në Irak. Qëllimi i studimit është t'u japë trupave një mënyrë të teknologjisë së lartë për t'u përballur dhe kapërcyer plagët mendore të luftës. Këtu me ndihmën e teknologjisë VR në mënyrë elektronike, krijohet një Irak virtual me efekte të shtuara të zërit, dritës dhe efekteve të tjera. Në këtë lloj terapie të ekspozimit, një terapist ndihmon ushtarakun të përballet me kujtimet, në mënyrë që ai ose ajo të ketë më pak frikë nga ato kujtime, duke qenë në gjendje ta shikojë situatën ndryshe dhe më racionalisht. Këtu prodhohen një shumëllojshmëri aromash, të këndshme dhe të pakëndshme. Era e zjarrit, dizelit, korditit, erës së trupit dhe gomës që digjet gjithashtu luan një rol për të lehtësuar kujtesën dhe përpunimin emocional. Avantazhi më i madh i një terapie të tillë është se ajo lejon përsëritjen e zonës së luftës në një mënyrë të sigurt që terapistët mund ta kontrollojnë.[13]

8. Realiteti virtual në luftë

Teknologët ushtarakë janë të mendimit se teknologjitë si RV kanë potencialin për të ripërcaktuar luftën moderne dhe ekziston nevoja për të hulumtuar më shumë për teknologji të tilla përtej ekranit të pilotit luftarak dhe aplikimeve mjekësore. Aktualisht, puna është në progres për zhvillimin e helmetave të ushtarëve që mund të komunikojnë me një server kryesor që mbledh dhe shpërndan tre informacione dimensionale në syzet e përdoruesit në kohë reale. Me ndihmën e një kodi ngjyrash, ushtarët do të paralajmëroheshin për gjëra të tilla si forcat miqësore, pikat e mundshme të rrezikut, vendet e afërta të sulmeve ajrore, pikat e takimit dhe shumë aspekte të tjera të rëndësishme. Gjithashtu, industria ushtarake amerikane po punon drejt zhvillimit të një sistemi censorësh dhe ekranesh të lehta që mbledh dhe ofron të dhëna nga dhe për çdo ushtar individual në terren. Kjo përfshin një kompjuter, një kamerë 360, sensorë UV dhe infra të kuqe, kamera stereoskopike dhe syze të tejdukshme të teknologjisë me diodë që lëshon dritë organike (OLED) (Cameron 2010). Teknologjia e robotikës është një teknologji ndërdisiplinore, e cila mund të lidhet me RV në një mënyrë të konsiderueshme dhe mund të përmirësojë dobinë e saj në trajnime me avionë, mbledhjen e inteligjencës, biomjekësore dhe aplikacione të ndryshme inxhinierike.

Industria e mbrojtjes në SHBA po punon në disa projekte, të bazuara në kërkesat e paraqitura nga ushtria. Qeveria amerikane po i mbështet sipërmarrjet e tilla. Që anëtarët e ekuipazhit të helikopterëve të ndërmarrin detyra specifike, bëhet esencial shkarkimi i të dhënave kompjuterike dhe grafika nga epokat e kamerave termike. Megjithatë, kryesisht nuk është e mundur të akomodohen monitorët tradicionalë për shkak të mungesës së hapësirës së mjaftueshme.

---

[13] http://www.stripes.com/news/military-uses-virtual-therapy-tohelp-troops-heal-ounds-1.929.

Përgjigja për këtë është përdorimi i një ekrani të montuar në kokë (HMD) i cili mund të kombinojë një monitor të vogël mbi sy, të montuar në një brez të rregullueshëm të veshur rreth kokës ose helmetës.

Natyrisht, pajisje të tilla pritet të përballojnë kushte të vështira, duke përfshirë klimat ekstreme, reshjet dhe pluhurin. Një HMD e tillë largohet nga një monitor tradicional në atë që ofron realitet të shtuar, që do të thotë se të dhënat e transmetuara shfaqen në mënyrë transparente në mënyrë që përdoruesi të mund të shohë përmes imazhit. Këtu imazhi është hedhur mbi pamjen e botës reale. Teknologjia HMD e realitetit të shtuar mund të luajë një rol të rëndësishëm në fushën e betejës digjitale të sotme. Ai ofron një zgjidhje për problemin e ekraneve jo të dukshme që pengojnë pamjen e një ushtari (Howard 2007).

Trajnimi i ushtarëve i bazuar në VR, lejon trajnimin e trupave duke krijuar zona të huaja në tokën e vet.[14] Pajisja e trajnimit virtual krijon një simulim realist të territorit jashtë shtetit për të përgatitur ushtarët për dislokimet e ardhshme ndërkombëtare. Sisteme të tilla si shërbime të shumta, ai lejon krijimin e një skenari të fushëbetejës me kundërshtarin dhe gjithashtu ndihmon në trajnimin e trupave për të vepruar në një skenar të mundshëm të misionit të OKB-së ose në ndonjë dislokim tjetër të përbashkët me trupat e shteteve të tjera.

Nga perspektiva e tregut, tregu i simulimit ushtarak dhe trajnimit virtual po rritet me shpejtësi. Sektori i tij po shfaqet me shpejtësi si një sektor i rëndësishëm në industrinë e mbrojtjes. Pritet që si shtete të fillojnë të reduktojnë shpenzimet e mbrojtjes përballë presioneve ekonomike ose do të përpiqej të riorganizonte prioritetet e trajnimit, teknologjisë dhe harduerit, simulimi ushtarak dhe trajnimi virtual do të rriteshin si një alternativë me kosto efektive.

Aktualisht, SHBA dominon tregun e simulimit ushtarak dhe trajnimit virtual. Por, kërkesa po rritet globalisht nga MB dhe Franca në Evropë dhe shtete si Arabia Saudite në Lindjen e Mesme. Kina dhe India identifikohen si dy tregjet vendimtare në zhvillim në të ardhmen me një rritje shumë të fortë të shpenzimeve.[15]

---

[14] Army Uses Virtual Soldier Training, 01 nëntor 2010, http://www.armedforces-int.com/news/army-uses-virtual-reality soldier-training.html.

[15] Sipas Raporteve të Kërkimit të Tregut të Mbrojtjes të titulluar 'Tregu i Simulimit Ushtarak dhe Trajnimit Virtual 2010-2020'. Ky raport është publikuar nga Companiesandmarkets.com është një grumbullues kryesor i informacionit të biznesit në internet. Informacioni është i disponueshëm në http://www.reportlinker.com/p096388/The-Military-Simulation-and Virtual – Training - Market Analysis.Htm l#ixzz1G09RZYAV

Pjekuria e mundshme e kësaj teknologjie në fushën ushtarake në vitet e ardhshme sjell gjithashtu në plan të parë nevojën për të adresuar çështjet e politikave (Wilson 2008) të cilat janë të dukshme sot dhe mund të shfaqen në të ardhmen. Për këtë qëllim, është e rëndësishme të vlerësohet fakti se RV dhe degët e lidhura të teknologjisë me të ka të ngjarë të gjejnë dobinë e tyre në fushën ushtarake shumë përtej qëllimeve të trajnimit. Aktualisht, nuk ka një strategji të dukshme globale për të gjykuar dobinë ushtarake dhe performancën e teknologjive ekzistuese dhe në zhvillim të RV. Ashtu si të gjitha teknologjitë e tjera të zhvilluara ushtarake, është thelbësore të krijohet kuptimi bazë në nivel global në lidhje me RV. Kjo ndodh sepse kur teknologji të tilla do të përdoren për qëllime operacionale do të lindte nevoja për të formuluar udhëzime specifike dhe gjithashtu mund të parashikoheshin disa ndryshime doktrinare si në nivele politikash ashtu edhe në nivele operacionale në varësi të statusit të teknologjisë në atë moment në kohë. Në një të ardhme të afërt mund të dalin në pah çështje të ndryshme në lidhje me standardizimin e kësaj teknologjie, cilat mund të jenë aspektet e drejta dhe të padrejta të kësaj teknologjie në varësi të normave të vendosura globale, natyrës së infrastrukturës teknologjike (komunikim/satelit/bazë në tokë) kërkohet për të administruar këtë teknologji etj.

Gjithashtu, mund të ketë probleme në lidhje me transferimin dhe shitjen ndërkombëtare të kësaj teknologjie. Aspektet e përdorimit të dyfishtë të kësaj teknologjie dhe shqetësimet e lidhura globale mund të shfaqen gjithashtu në të ardhmen e afërt.

9. Hulumtimet e fundit dhe të ardhshme

Rritja e RV për ushtritë duhet të shihet pak më ndryshe në krahasim me disa teknologji të tjera. Kjo është për shkak se RV nuk është në të vërtetë një teknologji platforme si avioni luftarak, anija ose një tank.

Është më shumë një teknologji e orientuar drejt aplikimit. Në të njëjtën kohë, induksioni i tij duhet të shihet pak më ndryshe në krahasim me teknologjitë e tjera të orientuara nga aplikacioni si teknologjia e informacionit (IT). Kjo për shkak se në rastin e IT, një nga zbatueshmërisë kryesore është rritja e efikasitetit të sistemeve ekzistuese, por induksioni i RV, në vende kërkon ndryshime strukturore dhe doktrinare. Gjithashtu, disa aplikacione VR dhe të bazuara në shkencë njohëse ngrenë çështje morale dhe më e rëndësishmja RV mbetet ende në fushën e zhvillimit të teknologjisë, veçanërisht në kontekstin ushtarak. Për shkak të këtyre arsyeve dhe faktorëve të tjerë si kostoja dhe njohuritë teknologjike, vetëm pak ushtarakë aktualisht po bëjnë përpjekje të përqendruara për të futur këtë teknologji.

Nga ana tjetër, nuk disponohet shumë informacion në literaturën me burim të hapur në lidhje me zbatueshmërinë ushtarake të kësaj teknologjie ndoshta për shkak të natyrës së qenësishme të sekretit ushtarak.

Hulumtimi në RV ushtarake duket se është ndërmarrë kryesisht nga SHBA dhe disa vende evropiane. Organizatat qeveritare si Laboratori i Kërkimeve Detare të SHBA dhe disa institute të tjera kërkimore ushtarake janë të përfshira në kryerjen e kërkimeve ushtarake RV. Ushtria Suedeze po bën disa kërkime inovative në RV. Puna po kryhet nga tre administrata ushtarake, FOI-Agjencia Suedeze e Kërkimeve të Mbrojtjes, FMV-Administrata Suedeze e Materialeve të Mbrojtjes dhe SNDC-Kolegji Suedez i Mbrojtjes Kombëtare. Për operacionet ushtarake në terrenin urban, ata kanë zhvilluar një hartë e cila ofron informacion tredimensional me disa funksionalitete operacionale që i jep operatorit mbështetje konjitive për vendimet. Harta të tilla kanë dobi si një informacion dhe ndihmë për vendimmarrje gjatë një ushtrimi ose si një mjet planifikimi dhe vlerësimi. Ata po punojnë gjithashtu për ushtarët e ardhshëm, forcat e krijuara nga kompjuteri, modelimin e sjelljes njerëzore dhe teknologjitë e simulatorëve të fluturimit (Borgvall dhe Lif 2011).

Siç u përmend në artikull më herët, një nga tendencat e rëndësishme RV për të ardhmen duhet të jetë përshtatja e lojërave video për qëllime ushtarake. Veçanërisht, industria moderne e lojërave po mban parasysh shpejtësinë në rritje të kompjuterëve shtëpiak për dizajnimin e lojërave (Haar 2011). Ata janë gjetur gjithashtu duke zhvilluar module lojërash më realiste për t'u kujdesur për rritjen e konkurrencës në treg. Për shkak të kësaj, diferenca midis lojërave dhe simulatorëve ushtarakë duket se po bie ngadalë. Pritet që në të ardhmen e afërt ushtarakët të zhvillojnë disa nga mjetet e tyre të bazuara në RV duke modifikuar lojërat e disponueshme për t'iu përshtatur kërkesave të tyre.

Aktualisht, hulumtimi është duke u ndërmarrë në fushën e Sistemit të Informacionit Gjeografik të Realitetit Virtual. Kjo gjeneratë e re e GIS, kombinon GIS tredimensionale, teknologjinë vizuale dhe teknologjinë e realitetit virtual. Ky sistem mund të jetë një përdorim i madh për menaxhimin e të dhënave, analizën dhe paraqitjen grafike të hapësirës tredimensionale (The Research of Virtual Reality Geographic Information System 2011). Ushtarakët mund ta përdorin këtë sistem duke zëvendësuar modelet e tyre ekzistuese dy dimensionale të të dhënave hapësinore GIS. Gjithashtu, pasi të zhvillohen plotësisht, ushtarakët mund të vendosin përballë teknologjisë VRGIS në mjetet e tyre të ndryshme harduerike dhe softuerike si kërkesa. Çdo kërkim i mëtejshëm në fushën RV në lidhje me aplikimet mjekësore do të kishte dobi për ushtritë. Disa kërkime specifike duhet të ndërmerren në këtë fushë për të përmbushur kërkesat ushtarake. Trajtimi i ankthit është i rëndësishëm veçanërisht për ushtarët e plagosur në luftëra ose gjatë trajtimit të detyrave të tjera të lidhura me sigurinë. Ekziston nevoja për të zhvilluar terapitë njohëse dhe të sjelljes duke mbajtur parasysh nevojat ushtarake. Gjithashtu, veçanërisht për parashutistët simulatorët e trajnimit të kërcimit janë duke u përdorur për shumë vite. Ato kanë ndihmuar ndjeshëm në minimizimin e dëmtimeve. Në shekullin e njëzet e një, rolet e ushtarakëve po ripërcaktohen vazhdimisht dhe po angazhohen për të trajtuar fatkeqësitë natyrore si tërmetet, cunami, fatkeqësitë bërthamore deri te operacionet antipiraterike. Në rrethana të tilla, është thelbësore të trajnohen trupat në mënyrë adekuate dhe VR mund të ofrojë zgjidhje novatore në këtë drejtim.

Përfundime

Me kalimin e viteve, ushtritë moderne gjenden gjithnjë e më shumë duke përdorur teknologjinë RV me sukses. Zhvillime të rëndësishme në fushën e teknologjisë së informacionit dhe komunikimit kanë sjellë zgjidhje të shpejtë në teknologjinë RV. Për gjithë këto vite, trajnimi ka një fushë ku RV ka gjetur dobi maksimale dhe e njëjta gjë do të vazhdojë edhe në të ardhmen e afërt. Megjithatë, kuptohet mirë se trajnimi virtual mund të mos jetë në gjendje të zëvendësojë stërvitjen fizike ose stërvitjen aktuale operacionale dhe përvojat e mbledhura gjatë ushtrimeve të ndryshme ushtarake, por megjithatë ai mund të luajë një rol të madh në aspekte të tjera të ndryshme të trajnimit si për shkak teknologjik ashtu edhe financiar. Përparësitë, rëndësia e RV ka të ngjarë të rritet, në të ardhmen e afërt shumë më tepër për një sërë arsyesh. Së pari, zhvillimet e shpejta në teknologji janë duke ofruar zgjidhje të reja pothuajse reale dhe duke vënë në dispozicion mjete të shumta për të përmbushur kërkesat e ndryshme ushtarake përtej trajnimit. Së dyti, sfidat ushtarake të shekullit të njëzet e një, janë konvencionale dhe asimetrike në natyrë, duke kërkuar evoluimin e teknologjive inovative për t'i adresuar ato dhe RV mund të ofrojë disa nga përgjigjet. Së treti, RV ofron zgjidhje pa shkaktuar asnjë humbje ose dëmtim te njerëzit dhe pajisjet. Së katërti, teknologjia tani është e disponueshme me një çmim të menaxhueshëm. Kompjuterët personalë të gjeneratës së tanishme kanë aftësitë e super kompjuterëve të dikurshëm. Aksesorë të ndryshëm të sofistikuar që kërkohen për përvojën e RV janë në dispozicion me çmime të përballueshme. Së pesti, suksesi i teknologjisë RV e mban plotësisht larg "rrëmujën" gjatë marrjes së vendimeve operacionale, sepse funksionon në dimensione të ndryshme njëkohësisht dhe vë në dispozicion vetëm ato të kërkuara.

Bibliografia

1. Anderson F, Annett M, Bischof WF (2011) Mbështetuni në Wii: rehabilitimi fizik me periferikë të realitetit virtual Wii. http://www. ncbi.nlm.nih.gov/pubmed/20543303. Botuar më 28 Shkurt 2011.
2. Aukstakalnis S, Blatner D (1992). Mirazhi i silikonit, arti dhe shkenca e realitetit virtual, Berkeley, CA, Peachpit Press siç citohet në http://www.

se.rit.edu/*jrv/research/ar/ introduction.html. Botuar më 21 Tetor 2010.

3. Blacklock J, Zalcman L (2003). Forca Ajrore Mbretërore Australiane, mjedisi ajror virtual, aftësia e trajnimit të përkohshëm. http://dspace. dsto. Defence. gov. au/dspac e /bitstream/1947/3400/1/DSTO-CR-0279% 20PR.pdf.
4. Boduch R (2010) Haptic Technology. www.ele.uri.edu/courses/ ele282/ F06/Rebecca_2.pdf. Botuar më 10 Dhjetor 2010.
5. Cameron C (2010) Realiteti i shtuar i shkallës ushtarake mund të ripërcaktojë luftën moderne. Shih: http://www.readwriteweb.com/ archives/military_grade_augmented_reality_could_redefine_modern_ warfare.php. Botuar më 23 Shkurt 2011.
6. Durlach NI, Mavor AS (eds) (1995) Realiteti virtual: sfidat shkencore dhe teknologjike, National Academy Press, Washington, Haar R (2011) Realiteti virtual në ushtri: e tashmja dhe e ardhmja.
7. http://referaat.cs.utwente.nl/documents/2005_03_CINTELLIGENT_ INTERACTION/2005_03_C_Haar,D. Wter Virtual _Reality_in_the_ Military_present_and_future.pdf. Botuar më 2 Prill 2011
8. Herrero P, de Antonio A (2005) Agjentë virtualë inteligjentë që vëzhgojnë në fushën e betejës. Virtual Real 8.
9. Howard CE (2007) Departamenti i Mbrojtjes investon në ofrimin e teknologjisë së realitetit të shtuar për ushtarët këmbësorë. Shih: http://www. ushtarakaerospace.com/index/display/articledisplay/291411/articles/ ushtarakaerospace ectronics/volume18/issue5/news/departamentii-mbrojtjes-investon-indisponingaugmented-reality-technology ushtarët në këmbë.html. Botuar më 7 Mars 2011.
10. Lok JJ (2001) Trajnimi i realitetit virtual. Jane’s International Defense Review, fq. 55–60.
11. Molloy F (2009) Bëjeni të vërtetë. http://www.fastthinking.com.au/the magazine/autumn-2009/make-it-real.aspx.
12. Pan Z, Shi J, Lu Q(2000).Realiteti virtual dhe aplikimet e tij në Kinë: një përmbledhje. Int J Virtual Real 4(3):1–5.
13. Peters TM (2000) Kirurgjia e drejtuar nga imazhi: nga rrezet X në realitetin virtual. Metodat Kompjuterike Biomech Biomed Eng. http:// www.imazheri.robarts.ca/igns/documents/XRVR.pdf.
14. Rheingold H (1992). Realiteti Virtual, Simon & Schuster, Nju Jork.
15. http://www.mortonheilig.com/SensoramaPatent.pdf dhe http:// en.wikipedia.org /wiki/Morton_Heilig. Botuar më 24 qershor 2010.
16. Riva G, Davide F, Ijsselsteijn WA (2003) Të jesh atje: konceptet, efektet dhe

matja e pranisë së përdoruesit në mjedise sintetike. Ios Press, Amsterdem.

17. Schonfeld E (2011) Realiteti i Shtuar Vs. Realiteti virtual: Cili është më real? Shih: http://techcrunch.com/2010/01/06/augmentedreality-vs-virtual-reality/ http://en.wikipedia.org/wiki/Augmented_reality. Botuar më 21 Nëntor 2010.
18. Strickland J (2010) Si funksionojnë aplikacionet ushtarake të realitetit virtual. Shih: http://science.howstuffworks.com/virtual-military.htm/printable. Botuar më 10 Dhjetor 2010 Strickland J (2011) Si funksionojnë aplikacionet ushtarake të realitetit virtual. http://science.howstuffworks.com/virtual-military.htm. Botuar më 12 Janar 2011.
19. Tamura H, Yamamoto H, Katayama A (2001) Realiteti i përzier: ëndrrat e së ardhmes shihen në kufirin midis botës reale dhe asaj virtuale. IEEE Comput Graph Appl.
20. Kërkimi i Sistemit të Informacionit Gjeografik të Realitetit Virtual (2011). http://www.gispark.net/3s-articles/3d-gis/the-research-ofvirtual-reality-geographic information-system.html. Botuar më 2 Prill 2011.
21. Wilson C (2008) Avatarët, teknologjia e realitetit virtual dhe ushtria amerikane: çështje të reja të politikave. www.fas.org/sgp/crs/natsec/RS22857.pdf. Botuar më 24 Shkurt 2011.
22. Wong V (2010) Simulimi i fluturimit: një aplikim i realitetit virtual.
23. Yin Y et al (2010) Aplikimi i realitetit virtual në simulatorin e kërkimit dhe shpëtimit detar. Int J Virtual Real 9(3):1926.